McAfee®

Total Protection 2007

Benutzerhandbuch

Inhalt

McAfee Total Protection 7

McAfee SecurityCenter 9

Funktionen ... 10
Verwenden von SecurityCenter ... 11
Header ... 11
Linke Spalte ... 11
Hauptbereich ... 12
Erläuterungen zu den SecurityCenter-Symbolen ... 13
Erläuterungen zum Schutzstatus ... 15
Beheben von Sicherheitsproblemen ... 21
Anzeigen der SecurityCenter-Informationen ... 22
Verwenden des Menüs "Erweitert" ... 23
Konfigurieren von SecurityCenter-Optionen ... 25
Konfigurieren des Schutzstatus ... 26
Konfigurieren von Benutzeroptionen ... 27
Konfigurieren der Update-Optionen ... 31
Konfigurieren von Alarmoptionen ... 37
Ausführen häufiger Tasks ... 39
Ausführen häufiger Tasks ... 39
Zuletzt aufgetretene Ereignisse anzeigen ... 40
Automatisches Warten Ihres Computers ... 41
Manuelles Warten Ihres Computers ... 42
Verwalten Ihres Netzwerks ... 44
Weitere Informationen zu Viren ... 44

McAfee QuickClean 45

Erläuterungen zu den QuickClean-Funktionen ... 46
Funktionen ... 46
Bereinigen Ihres Computers ... 47
Verwenden von QuickClean ... 49

McAfee Shredder 51

Erläuterungen zu den Funktionen von Shredder ... 52
Funktionen ... 52
Vernichten unerwünschter Dateien mit Shredder ... 53
Verwenden von Shredder ... 54

McAfee Network Manager 57

Funktionen ... 58
Erläuterung der Network Manager-Symbole ... 59
Erstellen eines verwalteten Netzwerks ... 61
Arbeiten mit der Netzwerkzuordnung ... 62
Anmelden am verwalteten Netzwerk ... 65
Remote-Verwaltung des Netzwerks ... 71
Überwachen des Status und der Berechtigungen ... 72
Beheben von Sicherheitslücken ... 75

McAfee VirusScan 77

Funktionen ... 78
Verwalten des Virenschutzes ... 81
Verwenden des Virenschutzes ... 82
Verwenden des Spyware-Schutzes ... 86
Verwenden von SystemGuards ... 87
Verwenden von Skriptprüfungen ... 97
Verwenden des E-Mail-Schutzes ... 98
Verwenden des Instant Messaging-Schutzes ... 100
Manuelles Prüfen des Computers ... 101
Manuelles Scannen ... 102
Verwalten von VirusScan ... 107
Verwalten vertrauenswürdiger Listen ... 108
Verw. isolierter Programme, Cookies und Dateien ... 109
Anzeigen zuletzt aufg. Ereignisse und Protokolle ... 111
Autom. Melden anonymer Informationen ... 112
Grundlegendes zu Sicherheitswarnungen ... 113
Zusätzliche Hilfe ... 115
Fragen und Antworten (FAQs) ... 116
Problembehandlung ... 118

McAfee Personal Firewall 121

Funktionen ... 122
Firewall starten ... 125
Firewall-Schutz aktivieren ... 125
Firewall-Schutz deaktivieren ... 126
Mit Warnungen arbeiten ... 127
Allgemeines zu Warnungen ... 128
Informationswarnungen verwalten ... 131
Warnungen während eines Spiels anzeigen ... 131
Informationswarnungen verbergen ... 132
Firewall-Schutz konfigurieren ... 133
Firewall-Sicherheitsstufen verwalten ... 134
Empfehlungen für Warnungen konfigurieren ... 138
Firewall-Sicherheit optimieren ... 140
Firewall sperren und wiederherstellen ... 144
Programme und Berechtigungen verwalten ... 147
Internetzugriff für Programme gewähren ... 148
Programmen nur den Zugriff auf ausgehende Verbindungen gewähren ... 152
Internetzugriff für Programme blockieren ... 155

Zugriffsberechtigungen für Programme entfernen ... 158
Weitere Informationen zu Programmen abrufen ... 159
Systemdienste verwalten ... 161
Systemdienstports konfigurieren ... 162
Computerverbindungen verwalten ... 167
Vertrauenswürdige Computerverbindungen ... 168
Sperren von Computerverbindungen ... 173
Protokollierung, Überwachung und Analyse ... 179
Ereignisprotokollierung ... 180
Mit der Statistik arbeiten ... 185
Internetverkehr verfolgen ... 186
Internetdatenverkehr überwachen ... 191
Weitere Informationen zu Internet Security ... 195
Hackerwatch-Lernprogramm starten ... 196

McAfee SpamKiller 197

Funktionen ... 198
Verwalten von Web-Mail-Konten ... 201
Hinzufügen von Web-Mail-Konten ... 202
Ändern von Web-Mail-Konten ... 204
Entfernen von Web-Mail-Konten ... 206
Verwalten der Filterung von Web-Mail-Konten ... 207
Verwalten von Freunden ... 209
Grundlegendes zum Verwalten von Freunden ... 210
Automatisches Aktualisieren von Freunden ... 212
Ändern von Filteroptionen ... 215
Ändern der Filterung von E-Mail-Nachrichten ... 216
Ändern der Vorgehensweise, wie Nachrichten verarbeitet werden ... 218
Filtern von Nachrichten mit Zeichensätzen ... 219
Melden von Spam-Nachrichten ... 220
Verwalten persönlicher Filter ... 221
Grundlagen zum Verwalten persönlicher Filter ... 222
Verwenden regulärer Ausdrücke ... 225
Verwalten von SpamKiller ... 231
Verwalten des Spam-Schutzes ... 232
Verwenden von Symbolleisten ... 233
Konfigurieren des Phishing-Schutzes ... 235
De-/Aktivieren des Phishing-Schutzes ... 236
Ändern von Phishing-Filteroptionen ... 237
Zusätzliche Hilfe ... 239
Fragen und Antworten (FAQs) ... 240

McAfee Privacy Service 243

Funktionen ... 244
Einrichten der Kindersicherung ... 245
Erstellen der Inhaltsklass.gruppe e. Benutzers ... 246
Festlegen der Cookie-Blockierungsebene eines Benutzers ... 248
Festlegen der Internet-Zugriffszeiten eines Benutzers ... 256
Blockieren von Websites ... 257
Zulassen von Websites ... 261
Zulassen, dass Websites Cookies platzieren ... 263
Blockieren potentiell anstößiger Web-Bilder ... 265

Schützen von Informationen im Internet 267
Blockieren von Anzeigen, Popups und Web-Bugs 268
Blockieren von persönlichen Informationen 270
Schützen von Kennwörtern 273
Einrichten des Kennwort-Tresors 274

McAfee Data Backup 279

Funktionen 280
Archivieren von Dateien 281
Festlegen von Archivoptionen 282
Ausführen von vollständigen Archivierungen und Schnellarchivierungen 287
Arbeiten mit archivierten Dateien 291
Verwenden des Explorers der lokale Archive 292
Wiederherstellen von archivierten Dateien 295
Verwalten von Archiven 298

McAfee Wireless Network Security 299

Funktionen 300
Wireless Network Security starten 302
Wireless Network Security starten 302
Wireless Network Security deaktivieren 303
Drahtlose Netzwerke schützen 305
Geschützte drahtlose Netzwerke einrichten 306
Computer zum geschützten drahtlosen Netzwerk hinzufügen 319
Drahtlosen Netzwerken verwalten 323
Verwalten drahtloser Netzwerke 324
Sicherheit für drahtloses Netzwerk verwalten 337
Konfigurieren von Sicherheitseinstellungen 338
Netzwerkschlüssel verwalten 343
Drahtlose Netzwerke überwachen 353
Drahtlose Netzwerkverbindungen überwachen 354
Geschützte drahtlose Netzwerke überwachen 360
Problembehandlung 365

McAfee EasyNetwork 383

Funktionen 384
EasyNetwork einrichten 385
Starten von EasyNetwork 386
Anmelden an einem verwalteten Netzwerk 387
Verwaltetes Netzwerk verlassen 391
Dateien freigeben und senden 393
Dateien freigeben 394
Senden von Dateien an andere Computer 397
Drucker freigeben 399
Mit freigegebenen Druckern arbeiten 400

Referenz 403

Glossar 404

Info zu McAfee 423

Copyright 424

Index 425

KAPITEL 1

McAfee Total Protection

McAfee Total Protection Suite bietet umfassenden Schutz für Ihre privaten Daten, Ihren Computer und Ihr drahtloses Netzwerk sowie die automatische Sicherung wichtiger Dateien. Genießen Sie das Internet sorgenfrei, während Sie surfen, shoppen, Ihre Bankgeschäfte erledigen, E-Mails lesen und Instant Messaging verwenden. Sie wissen, dass McAfee immer aktiviert ist, immer aktualisiert wird und Sie somit immer schützt. Der zuverlässige Schutz von McAfee blockiert Bedrohungen und hält Hacker automatisch ab, so dass Ihr Computer sauber und sicher bleibt. Überwachen und beheben Sie Sicherheitsprobleme auf Ihren Heimcomputern mit McAfee Network Manager. Geben Sie Dateien und Drucker auf Ihrem Netzwerk mit McAfee EasyNetwork problemlos frei. McAfee ermöglicht außerdem die einfache Kontrolle Ihres Sicherheitsstatus sowie das einfache Überprüfen auf Viren und Spyware und gewährleistet, dass Ihre Produkte dank dem neu gestalteten McAfee SecurityCenter stets auf dem neuesten Stand sind. Zusätzlich erhalten Sie automatisch mit Ihrem Abonnement die neueste Software und die neuesten Updates.

Total Protection enthält folgende Programme:

- SecurityCenter
- Privacy Service
- Shredder
- VirusScan
- Personal Firewall
- SpamKiller
- Datensicherung
- Drahtlossicherheit
- Network Manager
- EasyNetwork
- SiteAdvisor

KAPITEL 2

McAfee SecurityCenter

McAfee SecurityCenter ist eine benutzerfreundliche Umgebung, in der McAfee-Benutzer ihre Sicherheitsabonnements starten, verwalten und konfigurieren können.

SecurityCenter dient außerdem als Informationsquelle für Viruswarnungen, Produktinformationen, Support und Abonnementinformationen sowie als schnelle Verbindung zu den Tools und News auf der McAfee-Website.

In diesem Kapitel

Funktionen 10
Verwenden von SecurityCenter 11
Konfigurieren von SecurityCenter-Optionen 25
Ausführen häufiger Tasks 39

Funktionen

McAfee SecurityCenter bietet folgende neue Funktionen und Vorteile:

Neu entworfener Sicherheitsstatus

Vereinfacht es, den Sicherheitsstatus Ihres Computers zu prüfen, nach Updates zu suchen und potentielle Sicherheitsrisiken zu beseitigen.

Ständige Updates und Upgrades

Installiert automatisch tägliche Updates. Wenn eine neue Version von McAfee verfügbar wird, erhalten Sie diese während der Laufzeit Ihres Abonnements automatisch, so dass gewährleistet wird, dass Sie stets über den aktuellsten Schutz verfügen.

Warnungen in Echtzeit

Sicherheitswarnungen benachrichtigen Sie über den Ausbruch neuer Viren und Sicherheitsbedrohungen. Sie bieten auch Reaktionsoptionen zum Entfernen und Neutralisieren der Bedrohung und enthalten weitere Informationen dazu.

Umfassender Schutz

Eine Vielzahl von Erneuerungsoptionen, so dass Ihr McAfee-Schutz stets auf dem aktuellsten Stand ist.

Leistungs-Tools

Entfernt nicht verwendete Dateien, defragmentiert verwendete Dateien und verwendet die Systemwiederherstellung, um Ihren Computer auf höchstem Leistungsniveau zu halten.

Echte Online-Hilfe

Unterstützung von Experten für Computer-Sicherheit von McAfee über den Internet-Chat, per E-Mail oder das Telefon.

Schutz für sicheres Surfen

Das McAfee SiteAdvisor-Browser-Plugin hilft Ihnen, sofern installiert, sich vor Spyware, Spam, Viren und Online-Bedrohungen zu schützen, indem es Websites klassifiziert, die Sie besuchen, oder die in Ihren Web-Suchergebnissen angezeigt werden. Sie erhalten ausführliche Sicherheitsklassifizierungen, die belegen, wie eine Site beim Test der E-Mail-Praktiken, Downloads, Online-Zugehörigkeiten und Störungen, z. B. Popups und Nachverfolgungs-Cookies von Fremdherstellern, abgeschnitten hat.

KAPITEL 3

Verwenden von SecurityCenter

SecurityCenter wird über das McAfee SecurityCenter-Symbol im Windows-Benachrichtigungsbereich rechts neben der Taskleiste oder über Ihren Windows-Desktop gestartet.

Wenn Sie SecurityCenter öffnen, wird im Bereich "Home" der Schutzstatus Ihres Computers angezeigt, und Sie erhalten schnellen Zugriff auf Update-, Scan (falls McAfee VirusScan installiert ist) und andere häufig auftretende Tasks:

Header

Hilfe

Anzeigen der Hilfedatei zur Anwendung

Linke Spalte

Aktualisieren

Aktualisieren Sie Ihr Produkt, um zu gewährleisten, dass Ihr Computer vor den neuesten Bedrohungen geschützt ist.

Scannen

Falls McAfee VirusScan installiert ist, können Sie einen manuellen Scan Ihres Computers durchführen.

Häufige Tasks

Führen Sie häufig vorkommende Tasks aus, einschließlich der Rückkehr zu Ihrem Home-Bereich, des Anzeigens kürzlich aufgetretener Ereignisse, des Verwaltens Ihres Computer-Netzwerks (falls es sich um einen Computer mit Verwaltungskapazitäten für dieses Netzwerk handelt) und des Wartens Ihres Computers. Falls McAfee Data Backup installiert ist, können Sie auch Ihre Daten sichern.

Komponenten installiert

Hier sehen Sie, welche Sicherheitsdienste die Sicherheit Ihres Computers schützen.

Hauptbereich

Sicherheitsstatus

Unter **Bin ich geschützt** finden Sie die allgemeine Ebene für den Schutzstatus Ihres Computers. Darunter können Sie Details zu diesem Status nach der Schutzkategorie und dem Schutztyp anzeigen.

SecurityCenter-Informationen

Zeigen Sie an, wann die letzte Aktualisierung Ihres Computers stattgefunden hat, wann der letzte Scan durchgeführt wurde (falls McAfee VirusScan installiert ist) und wann Ihr Abonnement abläuft.

In diesem Kapitel

Erläuterungen zu den SecurityCenter-Symbolen.....13
Erläuterungen zum Schutzstatus.....15
Beheben von Sicherheitsproblemen 21
Anzeigen der SecurityCenter-Informationen 22
Verwenden des Menüs "Erweitert".....23

Erläuterungen zu den SecurityCenter-Symbolen

In Ihrem Windows-Benachrichtigungsbereich werden SecurityCenter-Symbole rechts neben der Taskleiste angezeigt. Verwenden Sie diese Symbole, um zu erkennen, ob Ihr Computer umfassend geschützt ist, ob gerade ein Scan durchgeführt wird (falls McAfee VirusScan installiert ist), ob Updates vorliegen, um kürzlich aufgetretene Ereignisse anzuzeigen, Ihren Computer zu warten und Support von der McAfee-Website zu erhalten.

Öffnen von SecurityCenter und Verwenden der zusätzlichen Funktionen

Wenn SecurityCenter ausgeführt wird, wird das SecurityCenter M-Symbol rechts neben der Taskleiste im Windows-Systembereich angezeigt.

So öffnen Sie SecurityCenter und verwenden die zusätzlichen Funktionen:

- Klicken Sie mit der rechten Maustaste auf das Hauptsymbol von SecurityCenter, und klicken Sie anschließend auf eine der folgenden Optionen:
  - SecurityCenter öffnen
  - Updates
  - Direkte Links

    Das Untermenü enthält Links zu "Home", "Kürzlich aufgetretene Ereignisse", "Netzwerk verwalten", "Computer warten" und "Datensicherung" (falls installiert).
  - Abonnement überprüfen

    (Dieses Element wird angezeigt, wenn mindestens ein Produkt-Abonnement abgelaufen ist.)
  - Upgrade Center
  - Kundendienst

Prüfen Ihres Schutzstatus

Wenn Ihr Computer nicht umfassend geschützt ist, wird das Symbol für den Schutzstatus rechts neben der Taskleiste im Windows-Systembereich angezeigt. Das Symbol kann je nach dem Schutzstatus rot oder gelb sein.

So prüfen Sie Ihren Schutzstatus:

- Klicken Sie auf das Symbol für den Schutzstatus, um SecurityCenter zu öffnen und etwaige Probleme zu beheben.

Prüfen des Status Ihrer Updates

Wenn Sie auf Updates prüfen, wird das Updates-Symbol rechts neben der Taskleiste im Windows-Systembereich angezeigt.

So prüfen Sie den Status Ihrer Updates:

- Zeigen Sie auf das Updates-Symbol, um den Status Ihrer Updates als Quickinfo anzuzeigen.

Erläuterungen zum Schutzstatus

Der Gesamtschutzstatus Ihres Computers wird im Abschnitt **Bin ich geschützt?** von SecurityCenter dargestellt.

Der Schutzstatus informiert Sie darüber, ob Ihr Computer umfassend gegen die neuesten Sicherheitsbedrohungen geschützt ist oder ob Probleme Ihre Aufmerksamkeit verlangen. Sie finden hier außerdem Informationen zur Behebung dieser Probleme. Wenn ein Problem mehr als eine Schutzkategorie betrifft, kann das Beheben dieses Problems dazu führen, dass mehrere Kategorien wieder den Status für umfassenden Schutz erreichen.

Zu den Faktoren für den Schutzstatus zählen externe Sicherheitsbedrohungen, die auf dem Computer installierten Sicherheitsprodukte, Produkte mit Zugriff auf das Internet sowie deren Konfiguration.

Standardmäßig werden diese nicht kritischen Sicherheitsprobleme ignoriert und nicht im Gesamtschutzstatus protokolliert, wenn Spam-Schutz oder Inhaltsblockierung nicht installiert sind. Wenn ein Sicherheitsproblem jedoch von einem Link **Ignorieren** begleitet wird, können Sie auswählen, ob das Problem ignoriert werden soll, wenn Sie sicher sind, dass Sie es nicht beheben möchten.

Bin ich geschützt?

Informationen zur Gesamtebene des Schutzstatus Ihres Computers finden Sie unter **Bin ich geschützt** in SecurityCenter.

- **Ja** wird angezeigt, wenn Ihr Computer umfassend geschützt ist (grün).
- **Nein** wird angezeigt, wenn Ihr Computer teilweise geschützt (gelb) oder nicht geschützt (rot) ist.

Um die meisten Sicherheitsprobleme automatisch zu lösen, klicken Sie neben dem Schutzstatus auf **Beheben**. Wenn jedoch ein oder mehrere Probleme weiterhin bestehen und Ihre Reaktion erfordern, klicken Sie auf den Link nach dem Problem, um die empfohlene Aktion auszuführen.

Erläuterungen zu den Schutzkategorien und -typen

Unter **Bin ich geschützt** in SecurityCenter können Sie Details zum Status anzeigen, aufgeschlüsselt nach den folgenden Schutzkategorien und -typen:

- Computer und Dateien
- Internet und Netzwerk
- E-Mail und IM
- Parental Controls

Die in SecurityCenter angezeigten Schutztypen hängen davon ab, welche Produkte installiert sind. Wenn beispielsweise der PC Health-Schutztyp angezeigt wird, ist die McAfee-Datensicherungssoftware installiert.

Wenn in einer Kategorie keine Sicherheitsprobleme vorliegen, ist der Status "grün". Wenn Sie auf eine grüne Kategorie klicken, wird rechts eine Liste der aktivierten Schutztypen angezeigt, gefolgt von einer Liste der bereits ignorierten Probleme. Wenn keine Probleme vorliegen, wird eine Virushinweis statt der Probleme angezeigt. Sie können auch auf **Konfigurieren** klicken, um Ihre Optionen für diese Kategorie zu ändern.

Wenn alle Schutztypen in einer Kategorie den Status "grün" aufweisen, ist der Status der Kategorie insgesamt "grün". Wenn alle Schutzkategorien den Status "grün" aufweisen, ist der Schutzstatus insgesamt "grün".

Wenn eine der Schutzkategorien den Status "gelb" oder "rot" aufweist, können Sie die Sicherheitsprobleme lösen, indem Sie sie beheben oder ignorieren, wodurch sich der Status in "grün" ändert.

Erläuterungen zum Schutz von Computer und Dateien

Die Schutzkategorie "Computer und Dateien" umfasst die folgenden Schutztypen:

- **Virenschutz**: Der Echtzeit-Scan-Schutz schützt Ihren Computer vor Viren, Würmern, Trojanern, verdächtigen Skripts, Hybridangriffen und anderen Bedrohungen. Das Programm führt automatische Scans durch und versucht, die Dateien zu säubern (einschließlich komprimierter .exe-Dateien, des Boot-Sektors, des Speichers und wichtiger Dateien), wenn Sie oder Ihr Computer darauf zugreifen.
- **Spyware-Schutz**: Der Spyware-Schutz dient zur raschen Erkennung, Blockierung und Entfernung von Spyware, Adware und anderen potentiell unerwünschten Programmen, die Ihre persönlichen Daten sammeln und ohne Ihre Zustimmung weiterleiten.
- **SystemGuards**: SystemGuards erkennt Änderungen auf Ihrem Computer und gibt ggf. eine Warnung aus. Sie können diese Änderungen prüfen und entscheiden, ob Sie sie erlauben möchten.
- **Windows-Schutz**: Der Windows-Schutz gibt den Status des Windows-Updates auf Ihrem Computer an. Wenn McAfee VirusScan installiert ist, steht außerdem der Pufferüberlaufschutz zur Verfügung.

Einer der Faktoren für den Schutz von Computer und Dateien sind externe Virusbedrohungen. Schützt beispielsweise Ihre Antivirensoftware Ihren Computer, wenn ein Virenausbruch stattfindet? Zu den weiteren Faktoren gehören die Konfiguration Ihrer Antivirensoftware und ob Ihre Software fortlaufend mit den neuesten Erkennungssignaturdateien aktualisiert wird, damit der Schutz Ihres Computers vor den neuesten Bedrohungen gewährleistet bleibt.

Öffnen des Konfigurationsbereichs für "Computer und Dateien"

Wenn unter **Computer & Dateien** keine Probleme vorliegen, können Sie den Konfigurationsbereich über den Informationsbereich öffnen.

So öffnen Sie den Konfigurationsbereich für "Computer und Dateien":

1. Klicken Sie im Home-Bereich auf **Computer & Dateien**.
2. Klicken Sie im rechten Bereich auf **Konfigurieren**.

Erläuterungen zum Schutz von Internet und Netzwerk

Die Schutzkategorie "Internet und Netzwerk" umfasst die folgenden Schutztypen:

- **Firewall-Schutz**: Der Firewall-Schutz schützt Ihren Computer vor Intrusionen und unerwünschtem Netzwerkverkehr. Gewährt alle eingehenden und ausgehenden Internetverbindungen.
- **Drahtloser Schutz**: Der drahtlose Schutz schützt Ihr privates drahtloses Netzwerk vor Intrusionen und Datenabfang. Wenn Sie jedoch derzeit mit einem externen drahtlosen Netzwerk verbunden sind, variiert Ihr Schutz in Abhängigkeit der Sicherheitsebene dieses Netzwerks.
- **Web-Browsing-Schutz**: Der Web-Browsing-Schutz verhindert, dass auf Ihrem Computer Werbung, Popups und Web-Bugs ausgeführt werden, während Sie im Internet surfen.
- **Phishing-Schutz**: Der Phishing-Schutz hilft dabei, betrügerische Websites zu blockieren, die über Hyperlinks in E-Mails und Instant Messages, Popups und anderen Quellen persönliche Informationen abrufen.
- **Personal Information Protection**: Personal Information Protection blockiert die Veröffentlichung wichtiger und vertraulicher Daten im Internet.

Öffnen des Konfigurationsbereichs für "Internet und Netzwerk"

Wenn unter **Internet & Netzwerk** keine Probleme vorliegen, können Sie den Konfigurationsbereich über den Informationsbereich öffnen.

So öffnen Sie den Konfigurationsbereich für "Internet und Netzwerk":

1. Klicken Sie im Home-Bereich auf **Internet & Netzwerk**.
2. Klicken Sie im rechten Bereich auf **Konfigurieren**.

Erläuterungen zu E-Mail- und IM-Schutz

Die Schutzkategorie "E-Mail- und IM-Schutz" umfasst die folgenden Schutztypen:

- **E-Mail-Schutz**: Der E-Mail-Schutz führt automatische Scans durch und versucht, Viren, Spyware und potentielle Bedrohungen in eingehenden und ausgehenden E-Mail-Nachrichten und -Anhängen zu säubern.
- **Spam-Schutz**: Der Spam-Schutz hilft Ihnen, Ihren E-Mail-Posteingang frei von unerwünschten E-Mails zu halten.
- **IM-Schutz**: Der Instant Messaging (IM)-Schutz führt automatische Scans durch und versucht, Viren, Spyware und potentielle Bedrohungen in eingehenden Instant Messaging-Nachrichten zu säubern. Das Programm verhindert außerdem, dass Instant Messaging-Clients unerwünschte Inhalte oder persönliche Informationen über das Internet austauschen.
- **Schutz für sicheres Surfen**: Falls installiert, hilft das McAfee SiteAdvisor-Browser-Plugin dabei, Ihren Computer vor Spyware, Spam, Viren und Online-Scams zu schützen, indem es Websites bewertet, die Sie besuchen oder die in Ihren Web-Suchergebnissen angezeigt werden. Sie können detaillierte Sicherheitsbewertungen anzeigen, aus denen hervorgeht, wie eine Site auf E-Mail-Praktiken, Downloads, Online-Partnerschaften und störende Praktiken, wie Popups und Verfolgungs-Cookies von Drittanbietern, getestet wird.

Öffnen des Konfigurationsbereichs für "E-Mail und IM"

Wenn unter **E-Mail & IM** keine Probleme vorliegen, können Sie den Konfigurationsbereich über den Informationsbereich öffnen.

So öffnen Sie den Konfigurationsbereich für "E-Mail und IM"

1. Klicken Sie im Home-Bereich auf **E-Mail & IM**.
2. Klicken Sie im rechten Bereich auf **Konfigurieren**.

Erläuterungen zum Parental Controls-Schutz

Die Schutzkategorie "Parental Controls" umfasst die folgenden Schutztypen:

- **Parental Controls**: Die Inhaltsblockierung verhindert, dass Benutzer unerwünschte Internet-Inhalte anzeigen, indem potentiell schädliche Websites blockiert werden. Die Internetaktivitäten und die -nutzung der Benutzer können außerdem überwacht und eingeschränkt werden.

Öffnen des Konfigurationsbereichs für "Parental Controls"

Wenn unter **Parental Controls** keine Probleme vorliegen, können Sie den Konfigurationsbereich über den Informationsbereich öffnen.

So öffnen Sie den Konfigurationsbereich für "Parental Controls":

1. Klicken Sie im Home-Bereich auf **Parental Controls**.
2. Klicken Sie im rechten Bereich auf **Konfigurieren**.

Beheben von Sicherheitsproblemen

Die meisten Sicherheitsprobleme können automatisch behoben werden. Wenn ein oder mehrere Probleme dennoch weiterhin vorliegen, müssen Sie sie lösen.

Automatisches Beheben von Sicherheitsproblemen

Die meisten Sicherheitsprobleme können automatisch behoben werden.

So beheben Sie Sicherheitsprobleme automatisch:

- Klicken Sie neben dem Schutzstatus auf **Beheben**.

Manuelles Beheben von Sicherheitsproblemen

Wenn ein oder mehrere Probleme nicht automatisch behoben werden, klicken Sie auf den Link nach dem Problem, um die empfohlene Aktion auszuführen.

So beheben Sie Sicherheitsprobleme manuell:

- Führen Sie einen der folgenden Vorgänge aus:
  - Wenn innerhalb der letzten 30 Tage kein vollständiger Scan Ihres Computers durchgeführt wurde, klicken Sie links neben dem HauptSchutzstatus auf **Scannen**, um einen manuellen Scan durchzuführen. (Dieses Element wird angezeigt, wenn McAfee VirusScan installiert ist.)
  - Wenn Ihre Virusdefinitionsdateien (DAT) veraltet sind, klicken Sie links neben dem HauptSchutzstatus auf **Update**, um Ihren Schutz zu aktualisieren.
  - Wennn ein Programm nicht installiert ist, klicken Sie für die Installation auf **Erhalten Sie vollständigen Schutz**.
  - Wenn Komponenten für ein Programm fehlen, installieren Sie es erneut.
  - Wenn ein Programm registriert sein muss, um vollständigen Schutz zu erhalten, klicken Sie zur Registrierung auf **Jetzt registrieren**. (Dieses Element wird angezeigt, wenn ein oder mehrere Programme abgelaufen sind.)
  - Wenn ein Programm abgelaufen ist, klicken Sie auf **Mein Abonnement jetz überprüfen**, um Ihren Kontostatus zu prüfen. (Dieses Element wird angezeigt, wenn ein oder mehrere Programme abgelaufen sind.)

Anzeigen der SecurityCenter-Informationen

Im unteren Teil des Schutzstatusbereichs bieten Ihnen die SecurityCenter-Informationen Zugriff auf SecurityCenter-Optionen. Sie sehen hier außerdem, wann das letzte Update sowie der letzte Scan durchgeführt wurden (falls McAfee VirusScan installiert ist) und wann die Abonnements für Ihre McAfee-Produkte ablaufen.

Öffnen des SecurityCenter-Konfigurationsbereichs

Sie können den SecurityCenter-Konfigurationsbereich öffnen, um Ihre Optionen im Home-Bereich zu ändern.

So öffnen Sie den SecurityCenter-Konfigurationsbereich:

- Klicken Sie im Home-Bereich unter **SecurityCenter-Informationen** auf die Option **Konfigurieren**.

Anzeigen von Informationen zum installierten Produkt

Sie können eine Liste der installierten Produkte anzeigen, in der Sie die Versionsnummer des Produkts und den Zeitpunkt der letzten Aktualisierung sehen.

So zeigen Sie Ihre McAfee-Produktinformationen an:

- Klicken Sie im Home-Bereich unter **SecurityCenter-Informationen** auf die Option **Details anzeigen**, um das Fenster mit Produktinformationen zu öffnen.

Verwenden des Menüs "Erweitert"

Wenn Sie SecurityCenter zum ersten Mal öffnen, wird in der linken Spalte das Menü "Grundlagen" angezeigt. Wenn Sie ein erfahrener Benutzer sind, können Sie auf das Menü **Erweitert** klicken, um ein detaillierteres Menü mit Befehlen an dieser Stelle anzuzeigen. Das zuletzt verwendete Menü wird angezeigt, wenn Sie SecurityCenter das nächste Mal verwenden.

Das Menü "Erweitert" umfasst die folgenden Elemente:

- Home
- Berichte und Protokolle (umfasst die Liste "Zuletzt aufgetretene Ereignisse" und Protokolle für die letzten 30, 60 und 90 Tage nach dem Typ geordnet)
- Konfigurieren
- Wiederherstellen
- Extras

KAPITEL 4

Konfigurieren von SecurityCenter-Optionen

SecurityCenter zeigt den Schutzstatus Ihres Computers insgesamt, ermöglicht Ihnen das Erstellen von McAfee-Benutzerkonten, installiert automatisch die neuesten Produkt-Updates und benachrichtigt Sie automatisch mit Warnmeldungen und -signalen bei öffentlichen Virenausbrüchen, Sicherheitsbedrohungen und Produkt-Updates.

Im SecurityCenter-Konfigurationsbereich können Sie Ihre SecurityCenter-Optionen für die folgenden Funktionen ändern:

- Schutzstatus
- Benutzer
- Automatische Updates
- Warnungen

In diesem Kapitel

Konfigurieren des Schutzstatus.....26
Konfigurieren von Benutzeroptionen.....27
Konfigurieren der Update-Optionen.....31
Konfigurieren von Alarmoptionen.....37

Konfigurieren des Schutzstatus

Der Gesamtschutzstatus Ihres Computers wird im Abschnitt **Bin ich geschützt?** von SecurityCenter dargestellt.

Der Schutzstatus informiert Sie darüber, ob Ihr Computer umfassend gegen die neuesten Sicherheitsbedrohungen geschützt ist oder ob Probleme Ihre Aufmerksamkeit verlangen. Sie finden hier außerdem Informationen zur Behebung dieser Probleme.

Standardmäßig werden diese nicht kritischen Sicherheitsprobleme ignoriert und nicht im Gesamtschutzstatus protokolliert, wenn Spam-Schutz oder Inhaltsblockierung nicht installiert sind. Wenn ein Sicherheitsproblem jedoch von einem Link **Ignorieren** begleitet wird, können Sie auswählen, ob das Problem ignoriert werden soll, wenn Sie sicher sind, dass Sie es nicht beheben möchten. Wenn Sie zu einem späteren Zeitpunkt beschließen, dass Sie ein zuvor ignoriertes Problem beheben möchten, können Sie das Problem zur Nachverfolgung in den Schutzstatus aufnehmen.

Konfigurieren ignorierter Probleme

Sie können Probleme als Teil des Schutzstatus Ihres Computers insgesamt in die Nachverfolgung aufnehmen oder davon ausschließen. Wenn ein Sicherheitsproblem von einem Link **Ignorieren** begleitet wird, können Sie auswählen, ob das Problem ignoriert werden soll, wenn Sie sicher sind, dass Sie es nicht beheben möchten. Wenn Sie zu einem späteren Zeitpunkt beschließen, dass Sie ein zuvor ignoriertes Problem beheben möchten, können Sie das Problem zur Nachverfolgung in den Schutzstatus aufnehmen.

So konfigurieren Sie ignorierte Probleme:

1. Klicken Sie unter **SecurityCenter-Informationen** auf **Konfigurieren**.
2. Klicken Sie auf den Pfeil neben **Schutzstatus**, um den Bereich zu erweitern, und klicken Sie anschließend auf **Erweitert**.
3. Führen Sie im Bereich "Ignorierte Probleme" einen der folgenden Schritte aus:
   - Um zuvor ignorierte Probleme in den Schutzstatus mit aufzunehmen, aktivieren Sie die entsprechenden Kontrollkästchen.
   - Um Probleme aus dem Schutzstatus auszuschließen, wählen Sie die entsprechenden Kontrollkästchen aus.
4. Klicken Sie auf **OK**.

Konfigurieren von Benutzeroptionen

Wenn Sie Programme von McAfee ausführen, für die Benutzerberechtigungen erforderlich sind, entsprechen diese Berechtigungen standardmäßig den Windows-Benutzerkonten auf diesem Computer. Um die Benutzerverwaltung für diese Programme einfacher zu gestalten, können Sie jederzeit dazu übergehen, McAfee-Benutzerkonten zu verwenden.

Wenn Sie zur Verwendung von McAfee-Benutzerkonten übergehen, werden bestehende Benutzernamen und -berechtigungen aus Ihrem Parental Controls-Programm automatisch importiert. Wenn Sie McAfee-Benutzerkonten das erste Mal verwenden, müssen Sie jedoch ein Administratorkonto erstellen. Danach können Sie mit der Erstellung und Konfigurierung anderer McAfee-Benutzerkonten beginnen.

Übergehen zur Verwendung von McAfee-Benutzerkonten

Standardmäßig werden Windows-Benutzerkonten verwendet. Beim Wechseln zu McAfee-Benutzerkonten ist das Erstellen von zusätzlichen Windows-Benutzerkonten jedoch nicht mehr erforderlich.

So gehen Sie zur Verwendung von McAfee-Benutzerkonten über:

1. Klicken Sie unter **SecurityCenter-Informationen** auf **Konfigurieren**.
2. Klicken Sie auf den Pfeil neben **Benutzer**, um den Bereich zu erweitern, und klicken Sie anschließend auf **Erweitert**.
3. Um McAfee-Benutzerkonten zu verwenden, klicken Sie auf **Wechseln**.

Wenn Sie zum ersten Mal McAfee-Benutzerkonten verwenden, müssen Sie ein Administratorkonto erstellen (Seite 28).

Erstellen eines Administratorkontos

Wenn Sie McAfee-Benutzerkonten das erste Mal verwenden, werden Sie aufgefordert, ein Administratorkonto zu erstellen.

So erstellen Sie ein Administratorkonto:

1. Geben Sie im Feld **Kennwort** ein Kennwort ein, und wiederholen Sie Ihre Eingabe im Feld **Kennwort bestätigen**.
2. Wählen Sie aus der Liste eine Frage zur Wiederbeschaffung des Kennworts aus, und geben Sie die Antwort auf die geheime Frage in das Kästchen **Antwort** ein.
3. Klicken Sie auf **Übernehmen**.

   Wenn Sie fertig sind, wird der Benutzerkontotyp im entsprechenden Feld mit den bestehenden Benutzernamen und -berechtigungen aus Ihrem Parental Controls-Programm aktualisiert, falls zutreffend. Wenn Sie zum ersten Mal Benutzerkonten konfigurieren, wird der Bereich "Benutzer verwalten" angezeigt.

Konfigurieren von Benutzeroptionen

Wenn Sie zur Verwendung von McAfee-Benutzerkonten übergehen, werden bestehende Benutzernamen und -berechtigungen aus Ihrem Parental Controls-Programm automatisch importiert. Wenn Sie McAfee-Benutzerkonten das erste Mal verwenden, müssen Sie jedoch ein Administratorkonto erstellen. Danach können Sie mit der Erstellung und Konfiguration anderer McAfee-Benutzerkonten beginnen.

So konfigurieren Sie Benutzeroptionen:

1. Klicken Sie unter **SecurityCenter-Informationen** auf **Konfigurieren**.
2. Klicken Sie auf den Pfeil neben **Benutzer**, um den Bereich zu erweitern, und klicken Sie anschließend auf **Erweitert**.
3. Klicken Sie unter **Benutzerkonten** auf **Hinzufügen**.
4. Geben Sie in das Feld **Benutzername** einen Benutzernamen ein.
5. Geben Sie im Feld **Kennwort** ein Kennwort ein, und wiederholen Sie Ihre Eingabe im Feld **Kennwort bestätigen**.
6. Wählen Sie das Kontrollkästchen **Startbenutzer** aus, wenn Sie diesen neuen Benutzer als Startbenutzer festlegen möchten, wenn SecurityCenter gestartet wird.
7. Wählen Sie unter **Benutzerkontotyp** einen Kontotyp für diesen Benutzer aus, und klicken Sie anschließend auf **Erstellen**.

   Hinweis: Nach dem Erstellen des Benutzerkontos müssen Sie unter "Parental Controls" die Einstellungen für einen Benutzer mit eingeschränkten Rechten konfigurieren.

8. Um das Kennwort eines Benutzers, die automatische Anmeldung oder den Kontotyp zu ändern, wählen Sie einen Benutzernamen aus der Liste aus, und klicken Sie auf **Bearbeiten**.
9. Klicken Sie auf **Übernehmen**.

Abrufen des Administratorkennworts

Wenn Sie das Administratorkennwort vergessen, können Sie es abrufen.

So rufen Sie das Administratorkennwort ab:

1. Klicken Sie mit der rechten Maustaste auf das SecurityCenter M-Symbol, und klicken Sie anschließend auf **Benutzer wechseln**.
2. Wählen Sie in der Liste **Benutzername** die Option **Administrator** aus, und klicken Sie anschließend auf **Kennwort vergessen**.
3. Geben Sie die Antwort auf die von Ihnen bei der Erstellung des Administratorkontos angegebene geheime Frage ein.
4. Klicken Sie auf **Senden**.

   Ihr vergessenes Administratorkennwort wird angezeigt.

Ändern des Administratorkennworts

Wenn Sie sich nicht an Ihr Administratorkennwort erinnern oder vermuten, dass es missbraucht worden sein könnte, können Sie es ändern.

So ändern Sie das Administratorkennwort:

1. Klicken Sie mit der rechten Maustaste auf das SecurityCenter M-Symbol, und klicken Sie anschließend auf **Benutzer wechseln**.
2. Wählen Sie in der Liste **Benutzername** die Option **Administrator** aus, und klicken Sie anschließend auf **Kennwort ändern**.
3. Geben Sie im Feld **Altes Kennwort** Ihr bestehendes Kennwort ein.
4. Geben Sie im Feld **Kennwort** das neue Kennwort ein, und wiederholen Sie Ihre Eingabe im Feld **Kennwort bestätigen**.
5. Klicken Sie auf **OK**.

Konfigurieren der Update-Optionen

SecurityCenter prüft nach Herstellung einer Internetverbindung automatisch alle vier Stunden auf Updates für Ihre gesamten McAfee-Dienste. Die neuesten Produkt-Updates werden anschließend automatisch installiert. Sie können auch jederzeit manuell prüfen, ob Updates vorliegen, indem Sie rechts neben der Taskleiste im Benachrichtigungsbereich auf das SecurityCenter-Symbol klicken.

Automatisches Prüfen auf Updates

Das Bestehen einer Internetverbindung vorausgesetzt, sucht SecurityCenter Online automatisch alle vier Stunden nach neuen Updates. Sie können SecurityCenter auch so konfigurieren, dass Sie benachrichtigt werden, bevor Updates heruntergeladen oder installiert werden.

So prüfen Sie automatisch auf Updates:

1. Klicken Sie unter **SecurityCenter-Informationen** auf **Konfigurieren**.
2. Klicken Sie auf den Pfeil neben **Automatische Updates aktiviert**, um den Bereich zu erweitern, und klicken Sie anschließend auf **Erweitert**.
3. Wählen Sie im Bereich "Update-Optionen" einen der folgenden Schritte aus:
   - Updates automatisch installieren und benachrichtigen, wenn das Produkt aktualisiert wurde (empfohlene Einstellung) (Seite 32)
   - Updates automatisch herunterladen und benachrichtigen, wenn das Installationsprogramm startbereit ist (Seite 33)
   - Vor dem Herunterladen von Updates benachrichtigen (Seite 34)
4. Klicken Sie auf **OK**.

Hinweis: Wenn Sie auf maximalen Schutz Wert legen, empfiehlt McAfee, dass Sie SecurityCenter automatisch nach Updates suchen und diese ggf. installieren lassen. Wenn Sie Ihre Sicherheitsdienste jedoch nur manuell aktualisieren möchten, können Sie die automatischen Updates deaktivieren (Seite 34).

Automatisches Herunterladen und Installieren von Updates

Wenn Sie in den SecurityCenter-Update-Optionen die Option **Updates automatisch installieren und benachrichtigen, wenn meine Dienste aktualisiert werden (empfohlene Einstellung)** auswählen, werden Updates automatisch von SecurityCenter heruntergeladen und installiert.

Automatisches Herunterladen von Updates

Wenn Sie in den Update-Optionen die Option **Updates automatisch herunterladen und benachrichtigen, wenn das Installationsprogramm startbereit ist** auswählen, lädt SecurityCenter Updates automatisch herunter und benachrichtigt Sie, wenn ein Update installiert werden kann. Sie können dann entscheiden, ob Sie das Update installieren oder die Installation auf einen späteren Zeitpunkt verschieben möchten (Seite 35).

So installieren Sie ein automatisch heruntergeladenes Update:

1. Klicken Sie in der Warnung auf **Meine Produkte jetzt aktualisieren** und anschließend auf **OK**.

   Bei entsprechender Aufforderung müssen Sie sich auf der Website anmelden, damit Ihr Abonnement verifiziert werden kann. Der Download erfolgt erst nach der Verifizierung.

2. Nach der Verifizierung Ihres Abonnements klicken Sie im Bereich "Updates" auf **Update**, um das Update herunterzuladen und zu installieren. Wenn Ihr Abonnement abgelaufen ist, klicken Sie in dem diesbezüglichen Warnhinweis auf **Abonnement erneuern** und folgen dann den Eingabeaufforderungen.

Hinweis: In einigen Fällen werden Sie aufgefordert, den Computer neu zu starten, um den Installationsvorgang für das Update abzuschließen. Speichern Sie Ihre Arbeit, und schließen Sie vor dem Neustart alle Programme.

Benachrichtigen vor dem Herunterladen von Updates

Wenn Sie im Bereich "Update-Optionen" **Benachrichtigen vor dem Herunterladen von Updates** aktiviert haben, werden Sie vor dem Herunterladen von Updates von SecurityCenter benachrichtigt. Sie können dann selbst entscheiden, ob Sie ein Update Ihrer Sicherheitsdienste herunterladen und installieren und damit die Gefahr eines Angriffs eliminieren möchten.

So laden und installieren Sie ein Update:

1. Klicken Sie in der Warnung auf **Meine Produkte jetzt aktualisieren** und anschließend auf **OK**.
2. Melden Sie sich bei der Website an, wenn Sie dazu aufgefordert werden.

   Das Update wird automatisch heruntergeladen.
3. Klicken Sie nach Abschluss der Update-Installation in der Warnung auf **OK**.

Hinweis: In einigen Fällen werden Sie aufgefordert, den Computer neu zu starten, um den Installationsvorgang für das Update abzuschließen. Speichern Sie Ihre Arbeit, und schließen Sie vor dem Neustart alle Programme.

Deaktivieren von automatischen Updates

Wenn Sie auf maximalen Schutz Wert legen, empfiehlt McAfee, dass Sie SecurityCenter automatisch nach Updates suchen und ggf. installieren lassen. Wenn Sie Ihre Sicherheitsdienste jedoch nur manuell aktualisieren möchten, können Sie die automatische Aktualisierung deaktivieren.

Hinweis: Prüfen Sie mindestens ein Mal wöchentlich, ob Updates verfügbar sind (Seite 36). Wenn Sie keine Updates installieren, sind die Sicherheitsmechanismen zum Schutz Ihres Computers nicht auf dem aktuellen Stand.

So deaktivieren Sie die automatische Aktualisierung:

1. Klicken Sie unter **SecurityCenter-Informationen** auf **Konfigurieren**.
2. Klicken Sie auf den Pfeil neben **Automatische Updates aktiviert**, um den Bereich zu erweitern.
3. Klicken Sie auf **Aus**.
4. Bestätigen Sie die Änderung, indem Sie auf **Ja** klicken.

   Der Status wird im Header aktualisiert.

Wenn Sie nach sieben Tagen nicht manuell prüfen, ob Updates zur Verfügung stehen, werden Sie durch eine Warnmeldung daran erinnert.

Verschieben von Updates auf einen späteren Zeitpunkt

Wenn Sie beim Empfang der Benachrichtigung zu beschäftigt sind, Ihre Sicherheitsdienste zu aktualisieren, können Sie wählen, ob Sie zu einem späteren Zeitpunkt daran erinnert werden möchten, oder die Nachricht ignorieren.

So verschieben Sie ein Update auf einen späteren Zeitpunkt:

- Führen Sie einen der folgenden Vorgänge aus:
  - Klicken Sie in der Warnung auf **Später erinnern** und anschließend auf **OK**.
  - Klicken Sie auf **Warnung schließen** und anschließend auf **OK**, um die Warnung zu schließen und keine Aktionen zu ergreifen.

Manuelles Prüfen auf Updates

SecurityCenter prüft nach Herstellung einer Internetverbindung automatisch alle vier Stunden auf Updates und installiert anschließend die neuesten Produkt-Updates. Sie können auch jederzeit manuell prüfen, ob Updates vorliegen, indem Sie rechts neben der Taskleiste im Windows-Benachrichtigungsbereich auf das SecurityCenter-Symbol klicken.

Hinweis: Wenn Sie auf maximalen Schutz Wert legen, empfiehlt McAfee, dass Sie SecurityCenter automatisch nach Updates suchen und diese ggf. installieren lassen. Wenn Sie Ihre Sicherheitsdienste jedoch nur manuell aktualisieren möchten, können Sie die automatischen Updates deaktivieren (Seite 34).

So prüfen Sie manuell auf Updates:

1. Stellen Sie sicher, dass Ihr Computer mit dem Internet verbunden ist.
2. Klicken Sie in Ihrem Windows-Benachrichtigungsbereich rechts neben der Taskleiste mit der rechten Maustaste auf das SecurityCenter M-Symbol und klicken Sie anschließend auf **Aktualisierungen**.

   Während SecurityCenter nach Updates sucht, können Sie weiterhin andere Aufgaben damit durchführen.

   Es wird in Ihrem Windows-Benachrichtigungsbereich rechts neben der Taskleiste ein animiertes Symbol angezeigt. Wenn SecurityCenter den Vorgang abgeschlossen hat, wird das Symbol automatisch wieder ausgeblendet.
3. Melden Sie sich bei der Website an, wenn Sie dazu aufgefordert werden, um Ihr Abonnement zu verifizieren.

Hinweis: In einigen Fällen werden Sie aufgefordert, den Computer neu zu starten, um den Installationsvorgang für das Update abzuschließen. Speichern Sie Ihre Arbeit, und schließen Sie vor dem Neustart alle Programme.

Konfigurieren von Alarmoptionen

Sie werden standardmäßig von SecurityCenter durch Warnmeldungen und akustische Warnsignale benachrichtigt, wenn Virusausbrüche stattfinden, Sicherheitsrisiken vorliegen oder Produkt-Updates verfügbar sind. Sie können SecurityCenter jedoch auch so konfigurieren, dass nur Warnungen angezeigt werden, die Ihre unmittelbare Aufmerksamkeit erfordern.

Konfigurieren von Warnoptionen

Sie werden standardmäßig von SecurityCenter durch Warnmeldungen und akustische Warnsignale benachrichtigt, wenn Virusausbrüche stattfinden, Sicherheitsrisiken vorliegen oder Produkt-Updates verfügbar sind. Sie können SecurityCenter jedoch auch so konfigurieren, dass nur Warnungen angezeigt werden, die Ihre unmittelbare Aufmerksamkeit erfordern.

So konfigurieren Sie Warnoptionen:

1. Klicken Sie unter **SecurityCenter-Informationen** auf **Konfigurieren**.
2. Klicken Sie auf den Pfeil neben **Warnungen**, um den Bereich zu erweitern, und klicken Sie anschließend auf **Erweitert**.
3. Wählen Sie im Bereich "Warnoptionen" einen der folgenden Schritte aus:
   - **Bei einem öffentlichen Virusausbruch oder einer öffentlichen Sicherheitsbedrohung benachrichtigen**
   - **Informationswarnungen einblenden, wenn Gaming-Modus erkannt wird**
   - **Akustisches Signal bei Warnungen ausgeben**
   - **Splash-Bildschirm von McAfee beim Starten von Windows anzeigen**
4. Klicken Sie auf **OK**.

Hinweis: Damit zukünftig keine informativen Warnmeldungen von der Warnung selbst mehr anzeigt werden, klicken Sie auf **Diese Warnung nicht mehr anzeigen**. Sie können diese Warnmeldungen später im Bereich "Informationswarnungen" erneut aktivieren.

Konfigurieren von Informationswarnungen

Informationswarnungen benachrichtigen Sie bei Ereignissen, die Ihr unmittelbares Eingreifen nicht erforderlich machen. Wenn Sie informative Warnmeldungen von der Warnung selbst für die Zukunft deaktivieren, können Sie sie später im Bereich "Informationswarnungen" erneut aktivieren.

So konfigurieren Sie Informationswarnungen:

1. Klicken Sie unter **SecurityCenter-Informationen** auf **Konfigurieren**.
2. Klicken Sie auf den Pfeil neben **Warnungen**, um den Bereich zu erweitern, und klicken Sie anschließend auf **Erweitert**.
3. Klicken Sie unter **SecurityCenter-Konfiguration** auf die Option **Informationswarnungen**.
4. Deaktivieren Sie das Kontrollkästchen **Informationswarnungen verbergen**, und deaktivieren Sie anschließend die Kontrollkästchen für Warnungen, die Sie anzeigen möchten, in der Liste.
5. Klicken Sie auf **OK**.

KAPITEL 5

Ausführen häufiger Tasks

Sie können häufig vorkommende Tasks ausführen, einschließlich der Rückkehr zu Ihrem Home-Bereich, des Anzeigens kürzlich aufgetretener Ereignisse, des Verwaltens Ihres Computer-Netzwerks (falls es sich um einen Computer mit Verwaltungskapazitäten für dieses Netzwerk handelt) und des Wartens Ihres Computers. Falls McAfee Data Backup installiert ist, können Sie auch Ihre Daten sichern.

In diesem Kapitel

Ausführen häufiger Tasks 39
Zuletzt aufgetretene Ereignisse anzeigen.....40
Automatisches Warten Ihres Computers 41
Manuelles Warten Ihres Computers.....42
Verwalten Ihres Netzwerks.....44
Weitere Informationen zu Viren 44

Ausführen häufiger Tasks

Sie können häufig vorkommende Tasks ausführen, einschließlich der Rückkehr zu Ihrem Home-Bereich, des Anzeigens kürzlich aufgetretener Ereignisse, des Wartens Ihres Computers und des Verwaltens Ihres Netzwerks (falls es sich um einen Computer mit Verwaltungskapazitäten für dieses Netzwerk handelt) und des Sicherns Ihrer Daten (falls McAfee Datensicherung installiert ist).

So führen Sie häufig vorkommende Tasks aus:

- Führen Sie im Menü "Grundlagen" unter **Häufige Tasks** einen der folgenden Schritte aus:
  - Um zum Home-Bereich zurückzukehren, klicken Sie auf **Home**.
  - Um kürzlich aufgetretene, von Ihrer Sicherheitssoftware erkannte Ereignisse anzuzeigen, klicken Sie auf **Zuletzt aufgetretene Ereignisse**.
  - Um nicht verwendete Dateien zu entfernen, Ihre Daten zu defragmentieren und Ihren Computer auf die vorherigen Einstellungen zurückzusetzen, klicken Sie auf **Computer warten**.
  - Um Ihr Computer-Netzwerk zu verwalten, klicken Sie auf einem Computer mit Verwaltungskapazitäten für dieses Netzwerk auf **Netzwerk verwalten**.

Der Network Manager überwacht PCs in Ihrem gesamten Netzwerk auf Sicherheitsschwachstellen, damit Sie Sicherheitsprobleme im Netzwerk einfach identifizieren können.

- Um Sicherungskopien Ihrer Dateien zu erstellen, klicken Sie auf **Datensicherung**, wenn McAfee Datensicherung installiert ist.

  Automatische Sicherungen speichern Kopien Ihrer wichtigsten Dateien, wann immer Sie möchten, so dass Ihre Dateien auf einem CD-/DVD-, USB- oder einem externen oder Netzwerklaufwerk verschlüsselt und gespeichert werden.

Tipp: Sie können häufig vorkommende Tasks von zwei weiteren Orten aus durchführen (unter **Home** im Menü "Erweitert" und im Menü **QuickLinks** des SecurityCenter M-Symbols ganz rechts auf der Taskleiste). Sie können unter **Berichte und Protokolle** im Menü "Erweitert" auch kürzlich aufgetretene Ereignisse und umfassende Protokolle nach Typ geordnet anzeigen.

Zuletzt aufgetretene Ereignisse anzeigen

Kürzlich aufgetreten Ereignisse werden protokolliert, wenn Änderungen an Ihrem Computer vorgenommen werden. Die Beispiele umfassen das Aktivieren oder Deaktivieren eines Schutztyps, das Entfernen einer Bedrohung sowie das Blockieren eines Versuchs, eine Internetverbindung herzustellen. Sie können die 20 am häufigsten aufgetretenen Ereignisse sowie die Details dazu anzeigen.

Details zu diesen Ereignissen finden Sie in der Hilfedatei des jeweiligen Produkts.

So zeigen Sie die zuletzt aufgetretenen Ereignisse an:

1. Klicken Sie mit der rechten Maustaste auf das SecurityCenter-Symbol, zeigen Sie auf **QuickLinks**, und klicken Sie anschließend auf **Aktuelle Ereignisse anzeigen**.

   Sämtliche kürzlich aufgetretenen Ereignisse werden in der Liste angezeigt, zusammen mit dem Datum und einer kurzen Beschreibung.

2. Wählen Sie unter **Zuletzt aufgetretene Ereignisse** ein Ereignis aus, um weitere Informationen im Detailbereich anzuzeigen.

   Unter **Ich möchte** werden alle verfügbaren Aktionen angezeigt.

3. Um eine umfassendere Liste mit Ereignissen anzuzeigen, klicken Sie auf **Protokoll anzeigen**.

Automatisches Warten Ihres Computers

Um wertvollen Speicherplatz auf Ihrer Festplatte frei zu machen und die Leistung Ihres Computers zu optimieren, können Sie QuickClean- oder Defragmentierungs-Task so planen, dass sie in regelmäßigen Zeitabständen ausgeführt werden. Diese Tasks umfassen das Löschen, Shreddern und Defragmentieren von Dateien und Ordnern.

So warten Sie Ihren Computer automatisch:

1. Klicken Sie mit der rechten Maustaste auf das SecurityCenter-Symbol, zeigen Sie auf **QuickLinks**, und klicken Sie anschließend auf **Computer warten**.
2. Klicken Sie auf **Taskplaner** auf **Start**.
3. Wählen Sie in der Vorgangsliste **QuickClean** oder **Defragmentierungsprogramm** aus.
4. Führen Sie einen der folgenden Vorgänge aus:
   - Um einen bestehenden Task zu verändern, wählen Sie den Task aus und klicken dann auf **Ändern**. Folgen Sie den Anweisungen auf dem Bildschirm.
   - Um einen neuen Task zu erstellen, geben Sie den Namen in das Feld **Taskname** ein und klicken anschließend auf **Erstellen**. Folgen Sie den Anweisungen auf dem Bildschirm.
   - Um einen Task zu löschen, wählen Sie ihn aus und klicken dann auf **Löschen**.
5. Zeigen Sie unter **Task-Zusammenfassung** an, wann der Task zuletzt ausgeführt wurde, wann er zum nächsten Mal ausgeführt wird sowie welchen Status er hat.

Manuelles Warten Ihres Computers

Sie können manuelle Wartungs-Tasks ausführen, um nicht verwendete Dateien zu entfernen, Ihre Daten zu defragmentieren und Ihren Computer auf die vorherigen Einstellungen zurückzusetzen.

So warten Sie Ihren Computer manuell:

- Führen Sie einen der folgenden Vorgänge aus:
  - Um QuickClean zu verwenden, klicken Sie mit der rechten Maustaste auf das SecurityCenter-Symbol, zeigen Sie auf **QuickLinks**, klicken Sie auf **Computer warten** und anschließend auf **Start**.
  - Um das Defragmentierungsprogramm zu verwenden, klicken Sie mit der rechten Maustaste auf das SecurityCenter-Symbol, zeigen Sie auf **QuickLinks**, klicken Sie auf **Computer warten**, und anschließend auf **Analysieren**.
  - Um die Systemwiederherstellung im Menü "Erweitert" zu verwenden, klicken Sie auf **Tools**, klicken Sie anschließend auf **Systemwiederherstellung** und dann auf **Start**.

Entfernen nicht verwendeter Dateien und Ordner

Verwenden Sie QuickClean, um wertvollen Speicherplatz frei zu machen und die Leistung Ihres Computers zu optimieren.

So entfernen Sie nicht verwendete Dateien und Ordner:

1. Klicken Sie mit der rechten Maustaste auf das SecurityCenter-Symbol, zeigen Sie auf **QuickLinks**, und klicken Sie anschließend auf **Computer warten**.
2. Klicken Sie unter **QuickClean** auf **Start**.
3. Folgen Sie den Anweisungen auf dem Bildschirm.

Defragmentieren von Dateien und Ordnern

Die Dateifragmentierung findet statt, wenn Dateien und Ordner gelöscht und neue Dateien hinzugefügt werden. Durch die Fragmentierung wird der Festplattenzugriff verlangsamt und die Gesamtleistung Ihres Computers herabgesetzt, wenn normalerweise auch nicht sehr stark.

Verwenden Sie das Defragmentierungsprogramm, um Teile einer Datei auf aufeinanderfolgenden Sektoren auf einer Festplatte zu schreiben, um die Geschwindigkeit von Zugriff und Abruf zu erhöhen.

So defragmentieren Sie Dateien und Ordner:

1. Klicken Sie mit der rechten Maustaste auf das SecurityCenter-Symbol, zeigen Sie auf **QuickLinks**, und klicken Sie anschließend auf **Computer warten**.
2. Klicken Sie unter **Defragmentierungsprogramm** auf **Analysieren**.
3. Folgen Sie den Anweisungen auf dem Bildschirm.

Zurücksetzen Ihres Computers auf die vorherigen Einstellungen

Wiederherstellungspunkte sind Kurzübersichten über Ihren Computer, die Windows in regelmäßigen Abständen speichert sowie wenn wichtige Ereignisse stattfinden (beispielsweise wenn ein Programm oder Treiber installiert wird). Sie können jdeoch auch jederzeit Ihre eigenen Wiederherstellungspunkte erstellen und diese benennen.

Verwenden Sie Wiederherstellungspunkte, um schädliche Änderungen an Ihrem Computer rückgängig zu machen und diesen auf die vorherigen Einstellungen zurückzusetzen.

So setzen Sie Ihren Computer auf die vorherigen Einstellungen zurück:

1. Klicken Sie im Menü "Erweitert" auf **Tools**, und klicken Sie anschließend auf **Systemwiederherstellung**.
2. Klicken Sie unter **Systemwiederherstellung** auf **Start**.
3. Folgen Sie den Anweisungen auf dem Bildschirm.

Verwalten Ihres Netzwerks

Wenn Ihr Computer über Verwaltungskapazitäten für Ihr Netzwerk verfügt, können Sie Network Manager verwenden, um PCs in Ihrem gesamten Netzwerk auf Sicherheitsschwachstellen zu überwachen, damit Sie Sicherheitsprobleme einfach identifizieren können.

Wenn der Schutzstatus Ihres Computers in diesem Netzwerk nicht überwacht wird, ist Ihr Computer entweder nicht Teil dieses Netzwerks, oder es handelt sich um ein nicht verwaltetes Mitglied dieses Netzwerks. Weitere Details hierzu finden Sie in der Hilfedatei zu Network Manager.

So verwalten Sie Ihr Netzwerk:

1. Klicken Sie mit der rechten Maustaste auf das SecurityCenter-Symbol, zeigen Sie auf **QuickLinks**, und klicken Sie anschließend auf **Netzwerk verwalten**.
2. Klicken Sie auf das Symbol, das in der Netzwerkkarte für diesen Computer steht.
3. Klicken Sie unter **Ich möchte** auf **Diesen Computer überwachen**.

Weitere Informationen zu Viren

Verwenden Sie die Vireninformationsbibliothek und die Virus Map, um folgende Aktionen durchzuführen:

- Erfahren Sie mehr zu den neuesten Viren, E-Mail-Virus-Hoaxes und anderen Bedrohungen.
- Erhalten Sie kostenlose Tools zur Virenentfernung, die Ihnen dabei helfen, Ihren Computer zu reparieren.
- Hier erfahren Sie aus der Vogelperspektive in Echtzeit, an welchen Orten der Welt derzeit PCs von Viren angegriffen werden.

So erhalten Sie weitere Informationen zu Viren:

1. Klicken Sie im Menü "Erweitert" auf **Tools**, und klicken Sie anschließend auf **Virusinformationen**.
2. Führen Sie einen der folgenden Vorgänge aus:
   - Untersuchen von Viren mithilfe der McAfee-Virusinformationsbibliothek
   - Untersuchen von Viren mithilfe der World Virus Map auf der McAfee-Website

KAPITEL 6

McAfee QuickClean

Beim Surfen im Internet sammelt sich viel Müll auf Ihrem Computer an. Schützen Sie Ihre Privatsphäre und löschen Sie Müll aus dem Internet und E-Mails, die Sie nicht benötigen, mit QuickClean. QuickClean identifiziert und löscht Dateien, die sich beim Internetsurfen angesammelt haben, einschließlich unerwünschter Cookies, E-Mails, Downloads und des Verlaufs - Daten, die persönliche Informationen über Sie enthalten. Es schützt Ihre Privatsphäre durch das sichere Löschen dieser sensiblen Informationen.

QuickClean löscht außerdem unerwünschte Programme. Legen Sie fest, welche Dateien eliminiert werden sollen, und sorgen Sie für Ordnung, ohne dabei wesentliche Informationen zu löschen.

In diesem Kapitel

Erläuterungen zu den QuickClean-Funktionen 46
Bereinigen Ihres Computers 47

Erläuterungen zu den QuickClean-Funktionen

In diesem Abschnitt werden die Funktionen von QuickClean beschrieben.

Funktionen

QuickClean bietet einen Satz an effizienten und leicht zu verwendenden Tools, mit denen digitale Überschussdaten sicher gelöscht werden können. Sie können wertvollen Festplattenspeicherplatz frei geben und die Leistung Ihres Computers optimieren.

KAPITEL 7

Bereinigen Ihres Computers

Mit QuickClean können Sie Dateien und Ordner sicher löschen.

Wenn Sie im Internet surfen, kopiert Ihr Browser jede Internetseite und die darin enthaltenen Graphiken in einen Ordner im Zwischenspeicher auf Ihrer Festplatte. Der Browser kann die Seite dann schnell herunterladen, wenn Sie auf diese Seite zurückkehren. Das Zwischenspeichern von Dateien ist nützlich, wenn Sie wiederholt dieselben Internetseiten besuchen und sich ihr Inhalt nicht häufig ändert. Meistens sind die zwischengespeicherten Dateien jedoch nicht hilfreich und können gelöscht werden.

Sie können verschiedene Elemente mit den folgenden Cleanern löschen.

- Papierkorb-Cleaner: Leert Ihren Windows-Papierkorb.
- Cleaner für temporäre Dateien: Löscht Dateien, die in temporären Ordner gespeichert sind.
- Kurzbefehls-Cleaner: Löscht unterbrochene Kurzbefehle und Kurzbefehle mit einem verknüpften Programm.
- Cleaner für verlorene Dateifragmente: Löscht verlorene Dateifragmente von Ihrem Computer.
- Registrierungs-Cleaner: Löscht Windows-Registrierungsinformationen für Programme, die von Ihrem Computer gelöscht wurden.
- Cache Cleaner: Entfernt Dateien aus dem Zwischenspeicher, die beim Browsen im Internet anfallen. Dateien dieses Typs werden in der Regel als temporäre Internet-Dateien gespeichert.
- Cookie Cleaner: Löscht Cookies. Dateien dieses Typs werden in der Regel als temporäre Internet-Dateien gespeichert. Cookies sind kleine Dateien, die Ihr Webbrowser auf Anfrage eines Webservers auf Ihrem Computer speichert. Wenn Sie danach erneut eine Seite dieser Website vom Webserver laden, sendet Ihr Browser das Cookie zurück an den Webserver. Diese Cookies können wie Tags fungieren, mit denen der Webserver nachverfolgen kann, welche Seiten wie oft aufgerufen wurden.
- Browser-Verlaufs-Cleaner: Löscht Ihren Browser-Verlauf.
- Outlook Express und Outlook E-Mail Cleaner für gelöschte und gesendete Elemente: Löscht E-Mails aus Ihren Ordnern für gesendete und gelöschte Outlook-E-Mails.
- Cleaner für zuletzt verwendete Dateien: Löscht kürzlich verwendete Elemente, die auf Ihrem Computer gespeichert sind, wie Microsoft Office-Dokumente.

- ActiveX und Plugin Cleaner: Löscht ActiveX-Steuerelemente und -Plugins.
  ActiveX ist eine Technologie, die für die Implementierung von Steuerelementen in ein Programm verwendet wird. Ein ActiveX-Steuerlement kann eine Schaltfläche zur Oberfläche eines Programms hinzufügen. Die meisten dieser Steuerelemente sind harmlos. Einige Personen verwenden jedoch die ActiveX-Technologie, um Informationen von Ihrem Computer zu sammeln.
  Plugins sind kleine Softwareprogramme, die eine Verbindung zu größeren Anwendungen herzustellen, um weitere Funktionen verfügbar zu machen. Plugins ermöglichen es dem Webbrowser, auf Dateien zuzugreifen und diese auszuführen, die in HTML-Dokumente eingebettet sind, die Formate aufweisen, die der Browser normalerweise nicht erkennen würde (beispielsweise Animations-, Video- und Audiodateien).
- Cleaner für Systemwiederherstellungspunkte: Löscht alte Systemwiederherstellungspunkte von Ihrem Computer.

In diesem Kapitel

Verwenden von QuickClean 49

Verwenden von QuickClean

In diesem Abschnitt wird beschrieben, wie QuickClean verwendet wird.

Säubern Ihres Computers

Sie können nicht verwendete Dateien und Ordner löschen, Festplattenspeicher freigeben und die Leistung Ihres Computers optimieren.

So säubern Sie Ihren Computer:

1. Klicken Sie im Menü "Erweitert" auf **Tools**.
2. Klicken Sie auf **Computer warten**, und klicken Sie anschließend unter **McAfee QuickClean** auf **Start**.
3. Führen Sie einen der folgenden Vorgänge aus:
   - Klicken Sie auf **Weiter**, um die in der Liste ausgewählten Standard-Cleaner zu übernehmen.
   - Wählen Sie die gewünschten Cleaner aus, und klicken Sie anschließend auf **Weiter.** Für den Cleaner für zuletzt verwendete Dateien können Sie auf **Eigenschaften** klicken, um die Programme zu löschen, deren Listen Sie nicht säubern möchten.
   - Klicken Sie auf **Standardwerte wiederherstellen**, um die Standard-Cleaner wiederherzustellen, und klicken Sie anschließend auf **Weiter**.
4. Klicken Sie nach Durchführung der Analyse auf **Weiter**, um das Löschen der Dateien zu bestätigen. Sie können diese Liste erweitern, um die Dateien anzuzeigen, die gesäubert werden, und deren Speicherort.
5. Klicken Sie auf **Weiter**.
6. Führen Sie einen der folgenden Vorgänge aus:
   - Klicken Sie auf **Weiter**, um den Standardwert **Nein, ich möchte meine Dateien mithilfe der Standardlöschung von Windows löschen** zu übernehmen.
   - Klicken Sie auf **Ja, ich möchte meine Dateien mit Shredder sicher löschen**, und geben Sie die Anzahl an Durchläufen an. Dateien, die mit Shredder gelöscht werden, können nicht wiederhergestellt werden.
7. Klicken Sie auf **Fertig stellen**.
8. Zeigen Sie unter **Zusammenfassung von QuickClean** die Anzahl an gelöschten Registrierungsdateien an sowie die Menge an Festplattenspeicher, der nach der Säuberung der Festplatte und der Internetdateien wieder zur Verfügug stand.

KAPITEL 8

McAfee Shredder

Gelöschte Dateien lassen sich auch nach dem Leeren des Papierkorbs wiederherstellen. Wenn eine Datei gelöscht wird, markiert Windows den betreffenden Speicherplatz auf dem Laufwerk als nicht mehr in Gebrauch, die Datei selbst ist jedoch noch vorhanden. Mit forensischen Computer-Tools können Steuererklärungen, Lebensläufe oder andere Dokumente, die von Ihnen gelöscht wurden, wiederhergestellt werden. Shredder schützt Ihre Privatsphäre, indem es unerwünschte Dateien permanent löscht.

Um eine Datei dauerhaft zu löschen, müssen Sie die vorhandene Datei wiederholt mit neuen Daten überschreiben. Microsoft(R) Windows löscht Dateien nicht sicher, da ansonsten sämtliche Dateivorgänge sehr langsam wären. Auch durch das Vernichten eines Dokuments wird nicht immer verhindert, dass das Dokument wiederhergestellt werden kann, da einige Programme temporäre verborgene Kopien geöffneter Dokumente erstellen. Wenn Sie nur die Dateien vernichten, die im Windows(R)-Explorer angezeigt werden, sind möglicherweise noch temporäre Kopien jener Dokumente irgendwo vorhanden.

Hinweis: Für vernichtete Dateien gibt es keine Sicherungskopien. Sie können von Shredder gelöschte Dateien nicht wiederherstellen.

In diesem Kapitel

Erläuterungen zu den Funktionen von Shredder 52
Vernichten unerwünschter Dateien mit Shredder ...53

Erläuterungen zu den Funktionen von Shredder

In diesem Abschnitt werden die Funktionen von Shredder beschrieben.

Funktionen

Shredder ermöglicht es Ihnen, den Inhalt Ihres Papierkorbs, temporäre Internetdateien, den Website-Verlauf, Dateien, Ordner und Datenträger wiederherzustellen.

KAPITEL 9

Vernichten unerwünschter Dateien mit Shredder

Shredder schützt Ihre persönlichen Daten, indem er unerwünschte Dateien, wie den Inhalt Ihres Papierkorbs, temporäre Internetdateien und den Website-Verlauf sicher und dauerhaft löscht. Sie können zu vernichtende Dateien und Ordner auswählen oder nach diesen suchen.

In diesem Kapitel

Verwenden von Shredder 54

Verwenden von Shredder

In diesem Abschnitt wird beschrieben, wie Shredder verwendet wird.

Vernichten von Dateien, Ordnern und Datenträgern

Dateien können auf Ihrem Computer verbleiben, auch nachdem Sie Ihren Papierkorb geleert haben. Wenn Sie jedoch Dateien vernichten, werden Ihre Daten dauerhaft gelöscht, und Hacker können nicht darauf zugreifen.

So vernichten Sie Dateien, Ordner und Datenträger:

1. Klicken Sie im Menü "Erweitert" auf **Tools**, und klicken Sie anschließend auf **Shredder**.
2. Führen Sie einen der folgenden Vorgänge aus:
   - Klicken Sie auf **Dateien und Ordner löschen**, um Dateien und Ordner zu vernichten.
   - Klicken Sie auf **Die Daten eines ganzen Datenträgers löschen**, um einen Datenträger zu vernichten**.**
3. Wählen Sie eine der folgenden Vernichtungsstufen aus:
   - **Schnell**: Vernichtet die ausgewählten Elemente in einem Durchlauf.
   - **Umfassend**: Vernichtet die ausgewählten Elemente in sieben Durchläufen.
   - **Benutzerdefiniert**: Vernichtet die ausgewählten Elemente in bis zu zehn Durchläufen. Eine hohe Anzahl an Vernichtungsdurchläufen erhöht Ihre Stufe für die sichere Dateientfernung.
4. Klicken Sie auf **Weiter**.
5. Führen Sie einen der folgenden Vorgänge aus:
   - Wenn Sie Dateien vernichten, klicken Sie in der Liste **Zu vernichtende Dateien auswählen** auf **Inhalt des Papierkorbs**, **Temporäre Internet-Dateien** oder **Website-Verlauf**. Wenn Sie einen Datenträger vernichten möchten, klicken Sie auf den Datenträger.
   - Klicken Sie auf **Durchsuchen**, navigieren Sie zu den zu vernichtenden Dateien, und wählen Sie sie aus.
   - Geben Sie den Pfad zu den zu vernichtenden Dateien in der Liste **Zu vernichtende Dateien auswählen** ein.

6 Klicken Sie auf **Weiter**.

7 Klicken Sie auf **Fertig stellen**, um den Vorgang abzuschließen.

8 Klicken Sie auf **Fertig**.

KAPITEL 10

McAfee Network Manager

McAfee(R) Network Manager stellt eine graphische Ansicht der Computer und Komponenten dar, die Ihr Home-Netzwerk bilden. Sie können Network Manager verwenden, um den Schutzstatus jedes verwalteten Computers in Ihrem Netzwerk remote zu überwachen und gemeldete Sicherheitslücken auf diesen verwalteten Computern remote zu beheben.

Bevor Sie mit der Verwendung von Network Manager beginnen, sollten Sie sich mit einigen der bekanntesten Funktionen vertraut machen. Details zur Konfiguration und Verwendung dieser Funktionen finden Sie in der Hilfe zu Network Manager.

In diesem Kapitel

Funktionen 58
Erläuterung der Network Manager-Symbole 59
Erstellen eines verwalteten Netzwerks 61
Remote-Verwaltung des Netzwerks 71

Funktionen

Network Manager bietet die folgenden Funktionen:

Graphische Netzwerkzuordnung

Die Netzwerkzuordnung von Network Manager bietet eine graphische Übersicht des Sicherheitsstatus der Computer und der Komponenten, aus denen Ihr privates Netzwerk besteht. Wenn Sie Änderungen an Ihrem Netzwerk vornehmen (wenn Sie beispielsweise einen Computer hinzufügen), erkennt die Netzwerkübersicht diese Änderungen. Sie können die Netzwerkzuordnung aktualisieren, das Netzwerk umbenennen und Komponenten der Netzwerkzuordnung anzeigen oder verbergen, um Ihre Ansicht anzupassen. Sie können auch die Details anzeigen, die mit den verschiedenen Komponenten verknüpft sind, die auf der Netzwerkzuordnung angezeigt werden.

Remote-Verwaltung

Verwenden Sie die Netzwerkübersicht von Network Manager zur Verwaltung des Sicherheitsstatus der Computer, aus denen Ihr privates Netzwerk besteht. Sie können einen Computer einladen, dem verwalteten Netzwerk beizutreten, den Schutzstatus des verwalteten Computers überwachen und bekannte Sicherheitslücken bei einem Remote-Computer im Netzwerk beheben.

Erläuterung der Network Manager-Symbole

Die folgende Tabelle erläutert die häufig auf der Network Manager-Netzwerkzuordnung verwendeten Symbole.

-Symbol	Beschreibung
	Steht für einen verwalteten Computer, der online ist.
	Steht für einen verwalteten Computer, der offline ist.
	Steht für einen unverwalteten Computer, auf dem die McAfee 2007-Sicherheits-Software installiert ist.
	Steht für einen unverwalteten Computer, der offline ist.
	Steht für einen Computer, der online ist und auf dem die McAfee 2007-Sicherheits-Software nicht installiert ist, oder für ein unbekanntes Netzwerkgerät.
	Steht für einen Computer, der offline ist und auf dem die McAfee 2007-Sicherheits-Software nicht installiert ist, oder für ein unbekanntes Netzwerkgerät, das offline ist.
	Bedeutet, dass das entsprechende Element geschützt und verbunden ist.
	Bedeutet, dass das entsprechende Element Ihrer Aufmerksamkeit bedarf.
	Bedeutet, dass das entsprechende Element Ihrer Aufmerksamkeit bedarf und keine Verbindung besteht.
	Steht für einen drahtlosen Home-Router.
	Steht für einen standardmäßigen Home-Router.
	Steht für das Internet, falls eine Verbindung besteht.
	Steht für das Internet, falls keine Verbindung besteht.

KAPITEL 11

Erstellen eines verwalteten Netzwerks

Sie erstellen ein verwaltetes Netzwerk, indem Sie mit den Elementen auf Ihrer Netzwerkzuordnung arbeiten und Mitglieder (Computer) zum Netzwerk hinzufügen.

In diesem Kapitel

Arbeiten mit der Netzwerkzuordnung.....62
Anmelden am verwalteten Netzwerk 65

Arbeiten mit der Netzwerkzuordnung

Jedes Mal, wenn Sie von einem Computer eine Verbindung zum Netzwerk herstellen, analysiert Network Manager den Status des Netzwerks, um festzustellen, ob Mitglieder vorliegen (verwaltet oder unverwaltet), welche Router-Attribute es gibt und wie der Internetstatus lautet. Wenn keine Mitglieder gefunden werden, nimmt Network Manager an, dass der derzeit verbundene Computer der erste Computer im Netzwerk ist, und macht den Computer automatisch zu einem verwalteten Mitglied mit Administratorrechten. Standardmäßig enthält der Name des Netzwerks den Arbeitsgruppen- oder Domänennamen des ersten Computers, auf dem die McAfee 2007-Sicherheits-Software installiert ist und der eine Verbindung zum Netzwerk herstellt. Sie können das Netzwerk jederzeit umbenennen.

Wenn Sie Änderungen an Ihrem Netzwerk vornehmen (wenn Sie beispielsweise einen Computer hinzufügen), können Sie die Netzwerkmappe an Ihre Bedürfnisse anpassen. Sie können beispielsweise die Netzwerkzuordnung aktualisieren, das Netzwerk umbenennen und Komponenten der Netzwerkzuordnung anzeigen oder verbergen, um Ihre Ansicht anzupassen. Sie können auch die Details anzeigen, die mit den verschiedenen Komponenten verknüpft sind, die auf der Netzwerkzuordnung angezeigt werden.

Zugreifen auf die Netzwerkzuordnung

Sie können auf Ihre Netzwerkzuordnung zugreifen, indem Sie Network Manager über die SecurityCenter-Liste der häufigen Tasks starten. Die Netzwerkzuordnung bietet eine graphische Darstellung des Computers und der Komponenten, die Ihr Home-Netzwerk ausmachen.

So greifen Sie auf die Netzwerkzuordnung zu:

- Klicken Sie im Menü "Grundlagen" oder "Erweitert" auf **Manage Network**.
  Die Netzwerkzuordnungen werden auf der rechten Seite angezeigt.

Hinweis: Wenn Sie das erste Mal auf die Netzwerkübersicht zugreifen, werden Sie gefragt, ob die anderen Computern im Netzwerk vertrauenswürdig sind, bevor die Netzwerkübersicht angezeigt wird.

Netzwerkzuordnung aktualisieren

Sie können die Netzwerkzuordnung jederzeit aktualisieren, beispielsweise wenn ein anderer Computer dem verwalteten Netzwerk beitritt.

So aktualisieren Sie die Netzwerkzuordnung:

1. Klicken Sie im Menü "Grundlagen" oder "Erweitert" auf **Manage Network**.
   Die Netzwerkzuordnungen werden auf der rechten Seite angezeigt.
2. Klicken Sie unter **Ich möchte** auf **Netzwerkzuordnung aktualisieren**.

Hinweis: Der Link **Netzwerkzuordnung aktualisieren** ist nur verfügbar, wenn in der Netzwerkzuordnung keine Elemente ausgewählt sind. Um die Auswahl eines Elements aufzuheben, klicken Sie auf das ausgewählte Element oder auf einen weißen Bereich in der Netzwerkzuordnung,

Netzwerk umbenennen

Standardmäßig enthält der Name des Netzwerks den Arbeitsgruppen- oder Domänennamen des ersten Computers, auf dem die McAfee 2007-Sicherheits-Software installiert ist und der eine Verbindung zum Netzwerk herstellt. Wenn dieser Name nicht passt, können Sie ihn ändern.

So benennen Sie das Netzwerk um:

1. Klicken Sie im Menü "Grundlagen" oder "Erweitert" auf **Manage Network**.
   Die Netzwerkzuordnungen werden auf der rechten Seite angezeigt.
2. Klicken Sie unter **Ich möchte** auf **Netzwerk umbenennen**.
3. Geben Sie im Feld **Netzwerk umbenennen** den Namen des Netzwerks ein.
4. Klicken Sie auf **OK**.

Hinweis: Der Link **Netzwerk umbenennen** ist nur verfügbar, wenn in der Netzwerkzuordnung keine Elemente ausgewählt sind. Um die Auswahl eines Elements aufzuheben, klicken Sie auf das ausgewählte Element oder auf einen weißen Bereich in der Netzwerkzuordnung,

Anzeigen oder Verbergen von Elementen in der Netzwerkzuordnung

Standardmäßig werden alle Computer und Komponenten in Ihrem Home-Netzwerk in der Netzwerkzuordnung angezeigt. Wenn Sie jedoch Elemente ausgeblendet haben, können Sie sie jederzeit wieder anzeigen. Nur unverwaltete Elemente können ausgeblendet werden, verwaltete Computer können nicht ausgeblendet werden.

Ziel	Klicken Sie im Menü "Grundlagen" oder "Erweitert" auf **Netzwerk verwalten**, und führen Sie anschließend die folgenden Schritte aus...
Verbergen eines Elements aus der Netzwerkzuordnung	Klicken Sie in der Netzwerkzuordnung auf ein Element, und klicken Sie anschließend unter **Ich möchte** auf **Dieses Element verbergen**. Klicken Sie im Dialogfeld für die Bestätigung auf **Ja**.
Anzeigen verborgener Elemente in der Netzwerkzuordnung	Klicken Sie unter **Ich möchte** auf **Verborgene Elemente anzeigen**.

Anzeigen der Elementdetails

Sie können detaillierte Informationen zu einer beliebigen Komponente in Ihrem Netzwerk anzeigen, indem Sie die Komponente in der Netzwerkzuordnung auswählen. Diese Informationen umfassen den Komponentennamen, seinen Schutzstatus und andere Informationen, die für die Verwaltung der Komponente erforderlich sind.

So zeigen Sie Details zu einem Element an:

1. Klicken Sie in der Netzwerkzuordnung auf das Symbol eines Elements.
2. Zeigen Sie unter **Details** die Informationen zu diesem Element an.

Anmelden am verwalteten Netzwerk

Bevor ein Computer remote verwaltet wird oder ihm Zugriff auf die Remote-Verwaltung anderer Computer im Netzwerk gewährt werden kann, muss er ein vertrauenswürdiges Mitglied des Netzwerks werden. Die Netzwerkmitgliedschaft wird neuen Computern von bestehenden Netzwerkmitgliedern (Computern) mit Administratorrechten gewährt. Um sicherzustellen, dass sich nur vertrauenswürdige Computer am Netzwerk anmelden, müssen sowohl Benutzer des gewährenden als auch des anzumeldenden Computers sich gegenseitig authentifizieren.

Wenn ein Computer dem Netzwerk beitritt, wird er aufgefordert, seinen McAfee-Schutzstatus für die anderen Computer im Netzwerk sichtbar zu machen. Wenn ein Computer zustimmt und seinen Schutzstatus sichtbar macht, wird er ein *verwaltetes* Mitglied des Netzwerks. Wenn ein Computer ablehnt und seinen Schutzstatus nicht sichtbar macht, wird er ein *unverwaltetes* Mitglied des Netzwerks. Unverwaltete Mitglieder des Netzwerks sind normalerweise Gastcomputer, die Zugriff auf andere Netzwerkfunktionen erlangen möchten (z. B. auf die Datei- oder Druckerfreigabe).

Hinweis: Wenn Sie andere Netzwerkprogramme von McAfee installiert haben (z. B. McAfee Wireless Network Security oder EasyNetwork), wird der Computer nach dem Beitritt auch in diesen Programmen als verwalteter Computer erkannt. Die Berechtigungsstufe, die einem Computer in Network Manager zugewiesen wird, gilt für alle McAfee-Netzwerkprogramme. Weitere Informationen dazu, was Gastberechtigungen, vollständige oder administrative Berechtigungen in anderen McAfee-Netzwerkprogrammen bedeuten, finden Sie in der Dokumentation zu dem jeweiligen Programm.

Anmelden an einem verwalteten Netzwerk

Wenn Sie eine Einladung erhalten, einem verwalteten Netzwerk beizutreten, können Sie diese entweder annehmen oder ablehnen. Sie können auch bestimmen, ob Sie möchten, dass dieser und andere Computer im Netzwerk gegenseitig ihre Sicherheitseinstellungen überwachen (beispielsweise ob die Virenschutzdienste eines Computers auf dem neuesten Stand sind).

So melden Sie sich an einem verwalteten Netzwerk an:

1. Aktivieren Sie im Dialogfeld für die Einladung das Kontrollkästchen **Es diesem und anderen Computern erlauben, gegenseitig ihre Sicherheitseinstellungen zu überwachen**, um es anderen Computern im verwalteten Netzwerk zu erlauben, die Sicherheitseinstellungen Ihres Computers zu überwachen.
2. Klicken Sie auf **Anmelden**.
   Wenn Sie die Einladung annehmen, werden zwei Spielkarten angezeigt.
3. Bestätigen Sie, dass die Spielkarten dieselben sind wie diejenigen, die auf dem Computer angezeigt werden, der Sie eingeladen hat, sich am verwalteten Netzwerk anzumelden.
4. Klicken Sie auf **Bestätigen**.

Hinweis: Wenn der Computer, der Sie eingeladen hat, sich am verwalteten Netzwerk anzumelden, nicht dieselben Spielkarten anzeigt, die auch im Dialogfeld für die Sicherheitsbestätigung angezeigt werden, liegt im verwalteten Netzwerk ein Sicherheitsverstoß vor. Durch das Anmelden am Netzwerk ist Ihr Computer möglicherweise einem Risiko ausgesetzt. Klicken Sie deshalb im Dialogfeld für die Bestätigung der Sicherheit auf **Ablehnen**.

Einladen eines Computers, sich am verwalteten Netzwerk anzumelden

Wenn ein Computer dem verwalteten Netzwerk hinzugefügt wird oder ein anderer unverwalteter Computer im Netzwerk vorliegt, können Sie diesen Computer einladen, sich am verwalteten Netzwerk anzumelden. Nur Computer mit Administratorrechten für das Netzwerk können andere Computer dazu einladen, sich am Netzwerk anzumelden. Wenn Sie die Einladung senden, können Sie auch die Berechtigungsstufe angeben, die Sie dem anzumeldenden Computer zuweisen möchten.

So laden Sie einen Computer ein, sich am verwalteten Netzwerk anzumelden:

1. Klicken Sie in der Netzwerkzuordnung auf das Symbol eines unverwalteten Computers.
2. Klicken Sie unter **Ich möchte** auf **Diesen Computer überwachen**.
3. Klicken Sie im Dialogfeld "Einen Computer einladen, diesem verwalteten Netzwerk beizutreten" auf eine der folgenden Optionen:
   - **Zugriff als Gast gewähren**
     Der Gastzugriff erlaubt dem Computer den Zugriff auf das Netzwerk.
   - **Vollständigen Zugriff auf alle verwalteten Netzwerkanwendungen gewähren**
     Mit dem vollständigen Zugriff (wie mit dem Gastzugriff) können Computer auf das Netzwerk zugreifen.
   - **Administrativen Zugriff auf alle verwalteten Netzwerkanwendungen gewähren**
     Mit dem administrativen Zugriff können Computer mit Administratorrechten auf das Netzwerk zugreifen. Dieser Zugriff erlaubt es dem Computer außerdem, anderen Computern Zugriff zu gewähren, die sich am verwalteten Netzwerk anmelden möchten.

4 Klicken Sie auf **Einladen**.
Es wird eine Einladung, dem verwalteten Netzwerk beizutreten, an den Computer gesendet. Wenn der Computer die Einladung annimmt, werden zwei Spielkarten angezeigt.

5 Bestätigen Sie, dass die Spielkarten dieselben sind wie diejenigen, die auf dem Computer angezeigt werden, den Sie eingeladen haben, sich am verwalteten Netzwerk anzumelden.

6 Klicken Sie auf **Zugriff gewähren**.

Hinweis: Wenn der Computer, den Sie eingeladen haben, sich am verwalteten Netzwerk anzumelden, nicht dieselben Spielkarten anzeigt, die auch im Dialogfeld für die Sicherheitsbestätigung angezeigt werden, liegt im verwalteten Netzwerk ein Sicherheitsverstoß vor. Wenn Sie es dem Computer erlauben, sich am Netzwerk anzumelden, werden dadurch andere Computer möglicherweise einem Risiko ausgesetzt. Klicken Sie deshalb im Dialogfeld für die Bestätigung der Sicherheit auf **Zugriff verweigern**.

Computer im Netzwerk nicht mehr als vertrauenswürdig einstufen

Wenn Sie fälschlicherweise zustimmen, den anderen Computern im Netzwerk zu vertrauen, so können Sie diese Auswahl auch wieder aufheben.

So erklären Sie Computer in diesem Netzwerk als nicht mehr vertrauenswürdig:

- Klicken Sie unter **Ich möchte** auf **Computern in diesem Netzwerk nicht mehr vertrauen**.

Hinweis: Der Link **Computern in diesem Netzwerk nicht mehr vertrauen** ist nur verfügbar, wenn sich keine anderen verwalteten Computer am Netzwerk angemeldet haben.

KAPITEL 12

Remote-Verwaltung des Netzwerks

Nachdem Sie Ihr verwaltetes Netzwerk eingerichtet haben, können Sie Network Manager verwenden, um die Computer und Komponenten, die sich in Ihrem Netzwerk befinden, remote zu verwalten. Sie können den Status und die Berechtigungsstufen der Computer und Komponenten überwachen und Sicherheitslücken remote beheben.

In diesem Kapitel

Überwachen des Status und der Berechtigungen 72
Beheben von Sicherheitslücken.....75

Überwachen des Status und der Berechtigungen

Ein verwaltetes Netzwerk hat zwei Arten von Mitgliedern: verwaltete Mitglieder und unverwaltete Mitglieder. Verwaltete Mitglieder erlauben es anderen Computern im Netzwerk, ihren McAfee-Schutzstatus einzusehen, unverwaltete Mitglieder tun das nicht. Unverwaltete Mitglieder sind normalerweise Gastcomputer, die Zugriff auf andere Netzwerkfunktionen erlangen möchten (z. B. auf die Datei- und Druckerfreigabe). Ein unverwalteter Computer kann jederzeit von einem anderen verwalteten Computer im Netzwerk eingeladen werden, ein verwalteter Computer zu werden. Ebenso kann ein verwalteter Computer jederzeit ein unverwalteter Computer werden.

Verwalteten Computern sind entweder administrative, vollständige oder Gastberechtigungen zugewiesen. Administrative Berechtigungen erlauben es dem verwalteten Computer, den Schutzstatus aller anderen verwalteten Computer im Netzwerk zu verwalten und anderen Computern die Mitgliedschaft im Netzwerk zu gewähren. Vollständige und Gastberechtigungen erlauben es einem Computer nur, auf das Netzwerk zuzugreifen. Sie können die Berechtigungsstufe eines Computers jederzeit ändern.

Da ein verwaltetes Netzwerk auch aus Geräten besteht (z. B. Routern), können Sie Network Manager auch für die Verwaltung dieser Geräte verwenden. Sie können auch die Anzeigeeigenschaften eines Geräts in der Netzwerkzuordnung konfigurieren und verändern.

Überwachen des Schutzstatus eines Computers

Wenn der Schutzstatus eines Computers nicht im Netzwerk überwacht wird (entweder, weil der Computer kein Mitglied des Netzwerks ist, oder weil der Computer ein unverwaltetes Mitglied des Netzwerks ist), können Sie eine Anfrage für die Überwachung stellen.

So überwachen Sie den Schutzstatus eines Computers:

1. Klicken Sie in der Netzwerkzuordnung auf das Symbol eines unverwalteten Computers.
2. Klicken Sie unter **Ich möchte** auf **Diesen Computer überwachen**.

Stoppen der Überwachung des Schutzstatus eines Computers

Sie können die Überwachung des Schutzstatus eines verwalteten Computers in Ihrem privaten Netzwerk stoppen. Der Computer wird dann zu einem unverwalteten Computer.

So stoppen Sie die Überwachung des Schutzstatus eines Computers:

1. Klicken Sie in der Netzwerkzuordnung auf das Symbol eines verwalteten Computers.
2. Klicken Sie unter **Ich möchte** auf **Diesen Computer nicht mehr überwachen**.
3. Klicken Sie im Dialogfeld für die Bestätigung auf **Ja**.

Ändern der Berechtigungen eines verwalteten Computers

Sie können die Berechtigungen eines verwalteten Computers jederzeit ändern. Dadurch können Sie angeben, welche Computer den Schutzstatus (Sicherheitseinstellungen) anderer Computer im Netzwerk überwachen können.

So ändern Sie die Berechtigungen eines verwalteten Computers:

1. Klicken Sie in der Netzwerkzuordnung auf das Symbol eines verwalteten Computers.
2. Klicken Sie unter **Ich möchte** auf **Berechtigungen für diesen Computer ändern**.
3. Aktivieren oder Deaktivieren Sie im Dialogfeld zum Ändern der Berechtigungen das Kontrollkästchen, das angibt, ob dieser Computer und andere Computer im verwalteten Netzwerk den Schutzstatus der anderen Computer überwachen können.
4. Klicken Sie auf **OK**.

Verwalten eines Geräts

Sie können ein Gerät verwalten, indem Sie von Network Manager aus auf ihre Verwaltungs-Website zugreifen.

So verwalten Sie ein Gerät:

1. Klicken Sie in der Netzwerkzuordnung auf das Symbol eines Geräts.
2. Klicken Sie unter **Ich möchte** auf **Dieses Gerät verwalten**. Es wird ein Webbrowser geöffnet, der die Verwaltungs-Webseite des Geräts anzeigt.
3. Geben Sie in Ihrem Webbrowser Ihre Anmeldeinformationen ein, und konfigurieren Sie die Sicherheitseinstellungen des Geräts.

Hinweis: Wenn es sich bei dem Gerät um einen durch Wireless Network Security geschützten drahtlosen Router oder Zugriffspunkt handelt, müssen Sie Wireless Network Security verwenden, um die Sicherheitseinstellungen eines Geräts zu konfigurieren.

Ändern der Anzeigeeigenschaften eines Geräts

Wenn Sie die Anzeigeeigenschaften eines Geräts verändern, können Sie den Anzeigenamen eines Geräts in der Netzwerkzuordnung ändern und angeben, ob es sich bei diesem Gerät um einen drahtlosen Router handelt.

So ändern Sie die Anzeigeeigenschaften eines Geräts:

1. Klicken Sie in der Netzwerkzuordnung auf das Symbol eines Geräts.
2. Klicken Sie unter **Ich möchte** auf **Geräteeigenschaften ändern**.
3. Um den Anzeigenamen des Geräts anzugeben, geben Sie einen Namen in das Feld **Name** ein.
4. Zum Angeben des Gerätetyps klicken Sie auf eine der folgenden Optionen:
   - **Router**
     Diese Option steht für einen standardmäßigen Home-Router.
   - **Drahtloser Router**
     Diese Option steht für einen drahtlosen Home-Router.
5. Klicken Sie auf **OK**.

Beheben von Sicherheitslücken

Verwaltete Computer mit Administratorrechten können den McAfee-Schutzstatus anderer verwalteter Computer im Netzwerk überwachen und sämtliche gemeldeten Sicherheitslücken remote beheben. Wenn beispielweise der McAfee-Schutzstatus eines verwalteten Computers angibt, dass VirusScan deaktiviert ist, kann ein anderer verwalteter Computer mit Administratorrechten diese Sicherheitslücke *beheben*, indem er VirusScan remote aktiviert.

Wenn Sie Sicherheitslücken remote beheben, repariert Network Manager automatisch die meisten gemeldeten Probleme. Einige Sicherheitslücken erfordern jedoch möglicherweise ein manuelles Eingreifen auf dem lokalen Computer. In diesem Fall behebt Network Manager diejenigen Probleme, die remote repariert werden können, und fordert Sie dann auf, die übrigen Probleme zu beheben, indem Sie sich auf dem betreffenden Computer bei SecurityCenter anmelden und die angegebenen Empfehlungen befolgen. In einigen Fällen lautet der Vorschlag, dass die McAfee 2007-Sicherheits-Software auf dem Remote-Computer oder den Computern in Ihrem Netzwerk installiert werden sollte.

Sicherheitslücken schließen

Sie können Network Manager verwenden, um automatisch die meisten Sicherheitslücken auf verwalteten Remote-Computern zu beheben. Wenn beispielsweise VirusScan auf einem Remote-Computer deaktiviert ist, können Sie für die automatische Aktivierung Network Manager verwenden.

So beheben Sie Sicherheitslücken:

1. Klicken Sie in der Netzwerkzuordnung auf das Symbol eines Elements.
2. Zeigen Sie unter **Details** den Schutzstatus eines Elements an.
3. Klicken Sie unter **Ich möchte** auf **Sicherheitslücken schließen**.
4. Klicken Sie auf **OK**, nachdem die Sicherheitslücken geschlossen wurden.

Hinweis: Auch wenn Network Manager die meisten Sicherheitslücken automatisch schließt, erfordert das Beheben einiger Probleme möglicherweise das Starten von SecurityCenter auf dem betroffenen Computer und das Befolgen der angegebenen Empfehlungen.

Installieren der McAfee-Sicherheits-Software auf Remote-Computern

Wenn auf einem oder meheren Computern in Ihrem Netzwerk die McAfee 2007-Sicherheits-Software nicht ausgeführt wird, kann ihr Schutzstatus nicht remote überwacht werden. Wenn Sie diese Computer remote überwachen möchten, müssen Sie zu jedem Computer gehen und die McAfee 2007-Sicherheits-Software installieren.

So installieren Sie die McAfee-Sicherheits-Software auf einem Remote-Computer:

1. Besuchen Sie in einem Browser auf dem Remote-Computer die Seite http://download.mcafee.com/us/.
2. Befolgen Sie die Bildschirmanweisungen für die Installation der McAfee 2007-Sicherheits-Software auf dem Computer.

KAPITEL 13

McAfee VirusScan

VirusScan bietet umfassenden, verlässlichen und aktuellen Schutz vor Viren und Spyware. Unterstützt durch die preisgekrönte McAfee-Scantechnologie schützt VirusScan vor Viren, Würmern, Trojanern, verdächtigen Skripts, Root-Kits, Pufferüberläufen, Hybridangriffen, Spyware, potentiell unerwünschten Programmen und anderen Bedrohungen.

In diesem Kapitel

Funktionen 78
Verwalten des Virenschutzes 81
Manuelles Prüfen des Computers 101
Verwalten von VirusScan 107
Zusätzliche Hilfe 115

Funktionen

Diese Version von VirusScan umfasst folgende Funktionen:

Virenschutz

Beim Echtzeit-Scan werden Dateien untersucht, wenn Sie oder Ihr Computer darauf zugreifen.

Scannen

Durchsucht Festplatten, Disketten sowie einzelne Dateien und Ordner nach Viren und anderen Bedrohungen. Sie können außerdem mit der rechten Maustaste auf ein Element klicken, um es zu untersuchen.

Erkennung von Spyware und Adware

VirusScan identifiziert und entfernt Spyware, Adware und andere Programme, die Ihre Privatsphäre verletzen und die Leistung Ihres Computers beeinträchtigen können.

Automatische Updates

Automatische Updates schützen Sie vor den neuesten identifizierten und nicht identifizierten Computerbedrohungen.

Schnelles Scannen im Hintergrund

Schnelle, im Hintergrund ausgeführte Scans identifizieren und beseitigen Viren, Trojaner, Spyware, Adware, Dialer und andere Bedrohungen, ohne Sie bei der Arbeit zu unterbrechen.

Echtzeit-Sicherheitswarnungen

Sicherheitswarnungen benachrichtigen Sie über den Ausbruch neuer Viren und Sicherheitsbedrohungen. Sie bieten auch Reaktionsoptionen zum Entfernen und Neutralisieren der Bedrohung und enthalten weitere Informationen dazu.

Erkennen und Säubern an den am meisten gefährdeten Stellen

VirusScan führt die Überwachung und Säuberung an den Haupteintrittspunkten des Computers durch: E-Mails, Instant Messaging-Anlagen und Internetdownloads.

Überwachung von E-Mails auf Aktivitäten, die auf einen Wurm hinweisen.

WormStopper™ blockiert Trojaner, die versuchen, Würmer per E-Mail an andere Computer zu senden, und fragt nach, bevor unbekannte E-Mail-Programme E-Mail-Nachrichten an andere Computer senden.

Überwachen von Skripts auf Aktivitäten, die auf einen Wurm hinweisen.

ScriptStopper™ blockiert bekannte, schädliche Skripts, so dass diese auf Ihrem Computer nicht ausgeführt werden.

McAfee X-Ray für Windows

McAfee X-Ray erkennt und entfernt Rootkits und andere Programme, die sich vor Windows verstecken.

Pufferüberlaufschutz

Der Pufferüberlaufschutz schützt Sie vor Pufferüberläufen. Pufferüberläufe passieren, wenn verdächtige Programme oder Prozesse versuchen, mehr Daten in einem Puffer (temporärer Speicher) zu speichern, als Ihr Computer zulässt, wodurch gültige Daten in nahe gelegenen Puffern beschädigt oder überschrieben werden.

McAfee SystemGuards

SystemGuards untersucht Ihren Computer auf bestimmte Verhaltensweisen, die auf Viren, Spyware oder Hacker-Aktivitäten hinweisen können.

KAPITEL 14

Verwalten des Virenschutzes

Sie können den Echtzeit-Viren-, Spyware-, SystemGuards- und Skriptschutz verwalten. Sie können beispielsweise das Scannen deaktivieren oder die zu scannenden Dateien angeben.

Die erweiterten Optionen können nur von Benutzern mit Administratorrechten geändert werden.

In diesem Kapitel

Verwenden des Virenschutzes 82
Verwenden des Spyware-Schutzes 86
Verwenden von SystemGuards 87
Verwenden von Skriptprüfungen.....97
Verwenden des E-Mail-Schutzes 98
Verwenden des Instant Messaging-Schutzes.....100

Verwenden des Virenschutzes

Wenn der Virenschutz (Echtzeit-Scannen) gestartet wird, überwacht er Ihrem Computer kontinuierlich auf Virusaktivitäten. Beim Echtzeit-Scannen werden alle Dateien gescannt, auf die Sie oder Ihr Computer zugreifen. Wenn der Virenschutz eine infizierte Datei erkennt, versucht er, die Infektion zu säubern oder zu entfernen. Wenn eine Datei nicht gesäubert oder entfernt werden kann, werden Sie in einer Warnmeldung zum Ausführen weiterer Maßnahmen aufgefordert.

Verwandte Themen

- Grundlegendes zu Sicherheitswarnungen (Seite 113)

Virenschutz deaktivieren

Wenn Sie den Virenschutz deaktivieren, wird Ihr Computer nicht mehr laufend auf Virenaktivitäten überprüft. Falls Sie den Virenschutz jedoch deaktivieren müssen, vergewissern Sie sich, dass keine Verbindung mit dem Internet besteht.

Hinweis: Durch die Deaktivierung des Virenschutzes wird auch der Spyware-, E-Mail- und Instant Messaging-Echtzeitschutz deaktiviert.

So deaktivieren Sie den Virenschutz:

1. Klicken Sie im Menü "Erweitert" auf **Konfigurieren**.
2. Klicken Sie im Konfigurationsbereich auf **Computer & Dateien**.
3. Klicken Sie unter **Virenschutz** auf **Aus**.
4. Führen Sie im Dialogfeld für die Bestätigung eine der folgenden Aktionen durch:
   - Wenn der Virenschutz nach einer bestimmten Zeit wieder aktiviert werden soll, aktivieren Sie das Kontrollkästchen **Echtzeit-Scan wieder aktivieren nach** und wählen Sie im Menü eine Uhrzeit aus.
   - Wenn der Virenschutz nicht nach einer bestimmten Zeit wieder aktiviert werden soll, deaktivieren Sie das Kontrollkästchen **Echtzeit-Scan wieder aktivieren nach**.

5 Klicken Sie auf **OK**.

Wenn der Echtzeitschutz so konfiguriert ist, dass er beim Start von Windows automatisch ausgeführt wird, ist Ihr Computer nach einem Neustart wieder geschützt.

Verwandte Themen

- Konfiguration des Echtzeitschutzes (Seite 84)

Aktivieren des Virenschutzes

Der Virenschutz überwacht Ihren Computer kontinuierlich auf Virusaktivitäten.

So aktivieren Sie den Virenschutz:

1 Klicken Sie im Menü "Erweitert" auf **Konfigurieren**.

2 Klicken Sie im Fenster "Konfigurieren" auf **Computer & Dateien**.

3 Klicken Sie unter **Virenschutz** auf **Ein**.

Konfigurieren des Echtzeit-Schutzes

Sie haben die Möglichkeit, den Echzeit-Virenschutz zu ändern. Sie können beispielsweise nur Programmdateien und -dokumente überprüfen lassen oder das Echtzeit-Scannen beim Starten von Windows deaktivieren (nicht empfohlen).

Konfiguration des Echtzeitschutzes

Sie können den Echtzeit-Virenschutz bearbeiten. Sie können beispielsweise festlegen, dass nur Programmdateien und Dokumente untersucht werden oder dass Echtzeit-Scans beim Starten von Windows deaktiviert werden (nicht empfohlen).

So konfigurieren Sie den Echtzeitschutz:

1. Klicken Sie im Menü "Erweitert" auf **Konfigurieren**.
2. Klicken Sie im Konfigurationsbereich auf **Computer & Dateien**.
3. Klicken Sie unter **Virenschutz** auf **Erweitert**.
4. Aktivieren oder deaktivieren Sie die folgenden Kontrollkästchen:
   - **Mithilfe von Heuristik auf unbekannte Viren prüfen**: Dateien werden mit Signaturen bekannter Viren verglichen, um Anzeichen nicht identifizierter Viren zu erkennen. Diese Option bietet die gründlichste Überprüfung, ist aber meist zeitaufwändiger als ein normaler Scan.
   - **Diskettenlaufwerk beim Herunterfahren prüfen**: Beim Herunterfahren Ihres Computers wird Ihr Diskettenlaufwerk untersucht.
   - **Auf Spyware und potentiell unerwünschte Programme prüfen**: Spyware, Adware und andere Programme, die potentiell ohne Ihre Erlaubnis Daten sammeln und übermitteln, werden erkannt und entfernt.
   - **Nachverfolgungs-Cookies suchen und entfernen**: Cookies, die potentiell ohne Ihre Erlaubnis Daten sammeln und übermitteln, werden erkannt und entfernt. Ein Cookie identifiziert Benutzer, wenn diese eine Webseite besuchen.
   - **Netzlaufwerke scannen**: Laufwerke, die mit Ihrem Netzwerk verbunden sind, werden gescannt.
   - **Pufferüberlaufschutz aktivieren**: Wenn eine Pufferüberlaufaktivität erkannt wird, wird sie blockiert, und Sie werden benachrichtigt.
   - **Echtzeit-Scans starten, wenn Windows gestartet wird (empfohlen)**: Der Echtzeitschutz wird bei jedem Start Ihres Computers aktiviert, auch wenn Sie ihn für eine Sitzung deaktivieren.

5 Klicken Sie auf eine der folgenden Schaltflächen:

- **Alle Dateien (empfohlen)**: Alle Dateitypen, die Ihr Computer verwendet, werden gescannt. Mit dieser Option erhalten Sie die gründlichste Überprüfung.
- **Nur Programmdateien und Dokumente**: Nur Programmdateien und Dokumente werden gescannt.

6 Klicken Sie auf **OK**.

Verwenden des Spyware-Schutzes

Der Spyware-Schutz entfernt Spyware, Adware und andere potenziell unerwünschte Programme, die Ihre Daten ohne Ihre Zustimmung sammeln und weiterleiten.

Deaktivieren des Spyware-Schutzes

Wenn Sie den Spyware-Schutz deaktivieren, werden potenziell unerwünschte Programme, die Ihre Daten ohne Ihre Zustimmung sammeln und weiterleiten, nicht erkannt.

So deaktivieren Sie den Spyware-Schutz:

1. Klicken Sie im Menü "Erweitert" auf **Konfigurieren**.
2. Klicken Sie im Fenster "Konfigurieren" auf **Computer & Dateien**.
3. Klicken Sie unter **Spyware-Schutz** auf **Aus**.

Aktivieren des Spyware-Schutzes

Der Spyware-Schutz entfernt Spyware, Adware und andere potenziell unerwünschte Programme, die Ihre Daten ohne Ihre Zustimmung sammeln und weiterleiten.

So aktivieren Sie den Spyware-Schutz:

1. Klicken Sie im Menü "Erweitert" auf **Konfigurieren**.
2. Klicken Sie im Fenster "Konfigurieren" auf **Computer & Dateien**.
3. Klicken Sie unter **Spyware-Schutz** auf **Ein**.

Verwenden von SystemGuards

SystemGuards erkennt nicht autorisierte Änderungen auf Ihrem Computer und gibt ggf. eine Warnung aus. Anschließend können Sie diese Änderungen prüfen und entscheiden, ob Sie sie zulassen oder nicht.

SystemGuards ist wie folgt kategorisiert.

Programm

SystemGuards für Programme erkennt Änderungen an Startdateien, Erweiterungen und Konfigurationsdateien.

Windows

SystemGuards für Windows erkennt Änderungen an Ihren Internet Explorer-Einstellungen, einschließlich der Browserattribute und Sicherheitseinstellungen.

Browser

SystemGuards für Browser erkennt Änderungen an Windows-Diensten, Zertifikaten und Konfigurationsdateien.

Deaktivieren von SystemGuards

Wenn Sie SystemGuards deaktivieren, werden nicht autorisierte Änderungen an Ihrem Computer nicht erkannt.

So deaktivieren Sie alle SystemGuards:

1. Klicken Sie im Menü "Erweitert" auf **Konfigurieren**.
2. Klicken Sie im Fenster "Konfigurieren" auf **Computer & Dateien**.
3. Klicken Sie unter **SystemGuard** auf **Aus**.

Aktivieren von SystemGuards

SystemGuards erkennt nicht autorisierte Änderungen auf Ihrem Computer und gibt ggf. eine Warnung aus.

So aktivieren Sie SystemGuards:

1. Klicken Sie im Menü "Erweitert" auf **Konfigurieren**.
2. Klicken Sie im Fenster "Konfigurieren" auf **Computer & Dateien**.
3. Klicken Sie unter **SystemGuard** auf **Ein**.

Konfigurieren von SystemGuards

Sie haben die Möglichkeit, SystemGuards zu konfigurieren. Sie können für jede erkannte Änderung festlegen, ob Sie benachrichtigt werden möchten und das Ereignis protokolliert, nur das Ereignis protokolliert oder SystemGuard deaktiviert werden soll.

Konfigurieren von SystemGuards

Sie haben die Möglichkeit, SystemGuards zu konfigurieren. Sie können für jede erkannte Änderung festlegen, ob Sie benachrichtigt werden möchten und das Ereignis protokolliert, nur das Ereignis protokolliert oder SystemGuard deaktiviert werden soll.

So konfigurieren Sie SystemGuards:

1. Klicken Sie im Menü "Erweitert" auf **Konfigurieren**.
2. Klicken Sie im Fenster "Konfigurieren" auf **Computer & Dateien**.
3. Klicken Sie unter **SystemGuard-Schutz** auf **Erweitert**.
4. Klicken Sie in der SystemGuards-Liste auf eine Kategorie, um eine Liste der zugeordneten SystemGuards und deren Status anzuzeigen.
5. Klicken Sie auf den Namen eines SystemGuard.
6. Unter **Details** finden Sie Informationen zu SystemGuard.
7. Führen Sie unter **Ich möchte** einen der folgenden Schritte aus:
   - Klicken Sie auf **Warnungen anzeigen**, wenn Sie benachrichtigt werden möchten, wenn eine Änderung eintritt und das Ereignis protokolliert wird.
   - Klicken Sie auf **Änderungen nur protokollieren**, wenn beim Erkennen einer Änderung keine Aktion ausgeführt werden soll. Die Änderung wird nur protokolliert.
   - Klicken Sie auf **Diesen SystemGuard deaktivieren**, um den SystemGuard zu deaktivieren. Sie werden im Fall einer Änderung weder benachrichtigt, noch wird das Ereignis protokolliert.
8. Klicken Sie auf **OK**.

Grundlegendes zu SystemGuards

SystemGuards erkennt nicht autorisierte Änderungen auf Ihrem Computer und gibt ggf. eine Warnung aus. Anschließend können Sie diese Änderungen prüfen und entscheiden, ob Sie sie zulassen oder nicht.

SystemGuards ist wie folgt kategorisiert.

Programm

SystemGuards für Programme erkennt Änderungen an Startdateien, Erweiterungen und Konfigurationsdateien.

Windows

SystemGuards für Windows erkennt Änderungen an Ihren Internet Explorer-Einstellungen, einschließlich der Browserattribute und Sicherheitseinstellungen.

Browser

SystemGuards für Browser erkennt Änderungen an Windows-Diensten, Zertifikaten und Konfigurationsdateien.

Allgemeines zu SystemGuards für Programme

SystemGuards für Programme erkennt folgende Elemente:

ActiveX-Installationen

Erkennt ActiveX-Programme, die über Internet Explorer heruntergeladen wurden. ActiveX-Programme werden von Websites heruntergeladen und auf dem Computer im Verzeichnis "C:\Windows\Downloaded Program Files" oder "C:\Windows\Temp\Temporary Internet Files" gespeichert. Zudem werden Sie in der Registrierung anhand ihrer CLSID (die lange Zahlenfolge zwischen den geschweiften Klammern) identifiziert.

Internet Explorer verwendet viele legitime ActiveX-Programme. Wenn Sie ein ActiveX-Programm nicht für vertrauenswürdig halten, können Sie es löschen, ohne dass dies Folgen für den Betrieb des Computers hat. Wenn Sie dieses Programm zu einem späteren Zeitpunkt wieder benötigen, lädt Internet Explorer es beim nächsten Mal herunter, wenn Sie eine Website öffnen, für die das Programm erforderlich ist.

Startelemente

Überwacht Änderungen an den Start-Registrierungschlüsseln und -ordnern. In den Start-Registrierungsschlüsseln der Windows-Registrierung und in den Startordnern im Startmenü werden die Pfade zu Programmen auf Ihrem Computer gespeichert. Die dort aufgeführten Programme werden beim Start von Windows geladen. Spyware oder andere potenziell unerwünschte Programme versuchen häufig zu starten, wenn Windows gestartet wird.

Windows Shell Execute Hooks

Überwacht Änderungen an der Liste der Programme, die in "explorer.exe" geladen werden. Ein Shell Execute Hook ist ein Programmm, das sich in die Windows-Shell von "explorer.exe" lädt. Ein Shell Execute Hook-Programm empfängt alle auf einem Computer ausgeführten Befehle. Jedes in die explorer.exe-Shell geladene Programm kann vor dem tatsächlichen Start eines weiteren Programms einen zusätzlichen Task ausführen. Spyware oder andere potenziell unerwünschte Programme können Shell Execute Hooks verwenden, um das Ausführen von Sicherheitsprogrammen zu verhindern.

Shell Service Object Delay Load

Überwacht Änderungen an Dateien, die im Registrierungsschlüssel "ShellServiceObjectDelayLoad" aufgelistet sind. Diese Dateien werden beim Starten des Computers von der Datei "explorer.exe" geladen. Da "explore.exe" die Shell des Computers ist, wird sie immer gestartet und lädt die unter diesem Registrierungsschlüssel aufgelisteten Dateien. Diese Dateien werden beim Startvorgang so frühzeitig geladen, dass der Benutzer nicht eingreifen kann.

Info zu Windows SystemGuards

Windows SystemGuards finden die folgenden Elemente:

Kontextmenü-Handler

Verhindert nicht genehmigte Änderungen der Windows-Kontextmenüs. Mittels dieser Menüs können Sie mit einem Klick der rechten Maustaste bestimmte Aktionen für diese Datei ausführen.

AppInit DLLs

Verhindert nicht genehmigte Änderungen oder Erweiterungen der AppInit.DLLs von Windows. Der Registrierungswert AppInit_DLLs enthält eine Liste der Dateien, die beim Laden der Datei user32.dll geladen werden. Dateien im Wert AppInit_DLLs werden ganz am Anfang der Windows-Startroutine geladen, wodurch möglicherweise schädliche DLLs verborgen werden, bevor ein Eingriff durch den Benutzer möglich ist.

Windows-Hostsdatei

Überwacht Änderungen an der Hostsdatei Ihres Computers. Ihre Hostsdatei wird zur Umleitung bestimmter Domänennamen an bestimmte IP-Adressen verwendet. Wenn Sie beispielsweise die Website www.beispiel.com besuchen, prüft der Browser die Hostsdatei, findet einen Eintrag für beispiel.com und verweist auf die IP-Adresse dieser Domäne. Einige Spyware-Programme versuchen, die Hostsdatei zu ändern, um den Browser zu einer anderen Website weiterzuleiten oder um zu verhindern, dass Software ordnungsgemäß aktualisiert wird.

Winlogon-Shell

Überwacht die Winlogon-Shell. Diese Shell wird automatisch geladen, wenn sich ein Benutzer bei Windows anmeldet. Bei dieser Shell handelt es sich um die Hauptbenutzeroberfläche (UI), die zur Verwaltung von Windows verwendet wird. In der Regel handelt es sich hierbei um den Windows-Explorer (explorer.exe). Die Windows-Shell kann jedoch leicht so geändert werden, dass sie auf ein anderes Programm verweist. In diesem Fall wird jedes Mal, wenn sich ein Benutzer anmeldet, ein anderes Programm als die Windows-Shell gestartet.

Windows-Anmeldung - Benutzerinitialisierung

Überwacht Änderungen an den Benutzereinstellungen der Windows-Anmeldung. Der Schlüssel HKLM\Software\Microsoft WindowsNT\CurrentVersion\Winlogon\Userinit legt fest, welches Programm gestartet wird, sobald sich ein Benutzer bei Windows anmeldet. Das Standardprogramm stellt das Profil, die Schriftarten, die Farben und andere Einstellungen für den Benutzernamen wieder her. Spyware und andere potentiell unerwünschte Programme können versuchen, sich selbst zu starten, indem sie sich selbst zu diesem Schlüssel hinzufügen.

Windows-Protokolle

Überwacht Änderungen an den Netzwerkprotokollen. Einige Spyware-Programme oder andere potentiell unerwünschte Programme übernehmen die Steuerung darüber, wie der Computer Informationen sendet und empfängt. Dies wird über die Windows-Protokollfilter und -handler erreicht.

Aufgesetzte Winsock-Dienstanbieter

Überwacht Layered Service Providers (LSPs), die Ihre Daten über das Netzwerk abrufen und sie ändern oder umleiten können. Legitime LSPs umfassen Software für Kindersicherungen, Firewalls und andere Sicherheitsprogramme. Spyware kann LSPs verwenden, um Ihre Internetaktivitäten zu überwachen und Ihre Daten zu bearbeiten. Um die Neuinstallation des Betriebssystems zu vermeiden, sollten Sie McAfee-Programme für das automatische Entfernen von Spyware und schadhaften LSPs verwenden.

Windows-Shell-Öffnungsbefehle

Verhindert Änderungen an den Öffnungsbefehlen der Windows-Shell (explore.exe). Shellöffnungsbefehle ermöglichen es einem bestimmten Programm, jedes Mal ausgeführt zu werden, wenn ein bestimmter Dateityp ausgeführt wird. Ein Wurm kann beispielsweise versuchen, jedes Mal ausgeführt zu werden, wenn eine EXE-Anwendung ausgeführt wird.

Gemeinsam verwendeter Taskplaner

Überwacht den Registrierungsschlüssel für den gemeinsam verwendeten Taskplaner, der eine Liste mit Programmen enthält, die beim Starten von Windows ausgeführt werden. Einige Spyware-Programme oder andere potentiell unerwünschte Programme ändern diesen Schlüssel und fügen sich ohne Ihre Erlaubnis selbst zur Liste hinzu.

Windows Messenger-Dienst

Überwacht den Windows Messenger-Dienst, der eine nicht dokumentierte Funktion von Windows Messenger ist, mit der Benutzer Popupmeldungen senden können. Einige Spyware-Programme oder andere potentiell unerwünschte Programme versuchen, den Dienst zu aktivieren und unerwünschte Werbung zu senden. Der Dienst kann auch durch Ausnutzen einer bekannten Sicherheitslücke bei remote ausgeführtem Code missbraucht werden.

Windows-Datei Win.ini

Die Datei Win.ini ist eine textbasierte Datei, die eine Liste der Programme enthält, die nach dem Starten von Windows ausgeführt werden sollen. Die Syntax zum Laden dieser Programme dient in dieser Datei zur Unterstützung älterer Windows-Versionen. Die meisten Programme verwenden zum Laden von Programmen nicht die Datei Win.ini: Einige Spyware-Programme oder andere potentiell unerwünschte Programme sind jedoch so konzipiert, dass sie sich diese Legacysyntax zunutze machen und beim Starten von Windows selbst laden.

Info zu Browser-SystemGuards

Windows SystemGuards finden die folgenden Elemente:

Browserhilfsobjekte

Überwacht Zusätze zu Browserhilfsobjekten (BHOs). Bei BHOs handelt es sich um Programme, die als Internet Explorer-Plugins fungieren. Spyware und Programme, die Ihren Browser missbrauchen, verwenden BHOs häufig, um Werbung anzuzeigen oder um Ihre Surfgewohnheiten zu verfolgen. BHOs werden auch von vielen legitimen Programmen verwendet, wie z. B. von gewöhnlichen Symbolleisten zum Suchen.

Internet Explorer-Leisten

Überwacht Änderungen, die an der Programmliste der Internet Explorer-Leiste vorgenommen werden. Bei Explorer-Leisten handelt es sich um Bereiche wie beispielsweise die Such-, Favoriten- oder Verlaufsbereiche, die in Internet Explorer (IE) oder Windows-Explorer angezeigt werden.

Internet Explorer-Plugins

Verhindert, dass Spyware Internet Explorer-Plugins installiert. Bei Internet Explorer-Plugins handelt es sich um Software-Addons, die beim Starten von Internet Explorer geladen werden. Spyware verwendet Internet Explorer-Plugins häufig, um Werbung anzuzeigen oder um Ihre Surfgewohnheiten zu verfolgen. Legitime Plugins fügen Funktionen zu Internet Explorer hinzu.

Internet Explorer-ShellBrowser

Überprüft Änderungen an Ihrer Internet Explorer-ShellBrowser-Instanz. Der Internet Explorer-ShellBrowser enthält Informationen und Einstellungen über eine Instanz von Internet Explorer. Falls diese Einstellungen geändert werden oder ein neuer ShellBrowser hinzugefügt wird, kann dieser ShellBrowser die Steuerung von Internet Explorer vollständig übernehmen und Funktionen wie beispielsweise Symbolleisten, Menüs und Schaltflächen hinzufügen.

Internet Explorer-Webbrowser

Überprüft Änderungen an Ihrer Internet Explorer-Webbrowser-Instanz. Der Internet Explorer-Webbrowser enthält Informationen und Einstellungen über eine Instanz von Internet Explorer. Falls diese Einstellungen geändert werden oder ein neuer Webbrowser hinzugefügt wird, kann dieser Webbrowser die Steuerung von Internet Explorer vollständig übernehmen und Funktionen wie beispielsweise Symbolleisten, Menüs und Schaltflächen hinzufügen.

Internet Explorer-URL-Suchhooks

Überwacht Änderungen, die am Internet Explorer-URL-Suchhook vorgenommen werden. URL-Suchhooks werden verwendet, wenn Sie eine Adresse im Adressfeld des Browsers ohne Verwendung von Protokollen (z. B. http:// oder ftp://) eingeben. Wenn Sie eine solche Adresse eingeben, kann der Browser URL-Suchhooks zum Durchsuchen des Internets nach der von Ihnen eingegebenen Adresse verwenden.

Internet Explorer-URLs

Überwacht Änderungen an den voreingestellten URLs von Internet Explorer. Dadurch wird verhindert, dass Spyware oder andere potentiell unerwünschte Programme Ihre Browser-Einstellungen ohne Ihre Zustimmung ändern.

Internet Explorer-Beschränkungen

Überwacht Internet Explorer-Beschränkungen, die es dem Computeradministrator ermöglichen, Benutzer daran zu hindern, die Startseite bzw. andere Optionen in Internet Explorer zu ändern. Diese Optionen sollten nur aktiviert sein, wenn sie der Administrator absichtlich festgelegt hat.

Internet Explorer-Sicherheitszonen

Überwacht Internet Explorer-Sicherheitszonen. Internet Explorer verfügt über vier vordefinierte Sicherheitszonen: Internet, lokales Intranet, vertrauenswürdige Sites und eingeschränkte Sites. Jede Sicherheitszone besitzt ihre eigene Sicherheitseinstellung, die vordefiniert ist oder vom Benutzer angepasst werden kann. Sicherheitszonen sind ein Ziel von einigen Spyware-Programmen oder anderen potentiell unerwünschten Programmen, da diese Programme durch das Herabsetzen der Sicherheitsstufe Sicherheitswarnungen umgehen und unerkannt handeln können.

Internet Explorer - Vertrauenswürdige Sites

Überwacht die vertrauenswürdigen Sites von Internet Explorer. Die Liste der vertrauenswürdigen Sites ist ein Verzeichnis der Websites, die Sie als vertrauenswürdig eingestuft haben. Diese Liste ist das Ziel von einigen Spyware-Programmen oder anderen potentiell unerwünschten Programmen, da verdächtige Sites damit ohne Ihre Erlaubnis im Vorhinein als vertrauenswürdig eingestuft werden können.

Internet Explorer-Richtlinie

Überwacht die Internet Explorer-Richtlinien. Diese Einstellungen werden normalerweise von Systemadministratoren verwendet, können aber durch Spyware missbraucht werden. Änderungen können verhindern, dass Sie eine andere Startseite festlegen, oder bewirken, dass Registerkarten im Dialogfeld "Internetoptionen" im Menü "Extras" nicht angezeigt werden.

Verwenden von Skriptprüfungen

Ein Skript kann Dateien erstellen, kopieren oder löschen. Es kann zudem die Windows-Registrierung öffnen.

Die Skriptprüfung verhindern automatisch, dass gefährliche Skripts auf Ihrem Computer ausgeführt werden.

Skriptprüfungen deaktivieren

Wenn Sie Skriptprüfungen deaktivieren, wird das Ausführen verdächtiger Skripts nicht erkannt.

So deaktivieren Sie Skriptprüfungen:

1. Klicken Sie im Menü "Erweitert" auf **Konfigurieren**.
2. Klicken Sie im Fenster "Konfigurieren" auf **Computer & Dateien**.
3. Klicken Sie unter **Skriptptüfung** auf **Aus**.

Prüfskripte aktivieren

Die Skriptptüfung gibt eine Warnmeldung aus, wenn die Ausführung eines Skripts dazu führt, dass Dateien erstellt, kopiert oder gelöscht werden, oder dass Ihre Windows-Registrierung geöffnet wird.

So aktivieren Sie Skriptprüfungen:

1. Klicken Sie im Menü "Erweitert" auf **Konfigurieren**.
2. Klicken Sie im Fenster "Konfigurieren" auf **Computer & Dateien**.
3. Klicken Sie unter **Skriptptüfung** auf **Ein**.

Verwenden des E-Mail-Schutzes

Der E-Mail-Schutz erkennt und blockiert Bedrohungen in eingehenden (POP3) und ausgehenden (SMTP) E-Mail-Nachrichten und Anhängen. Dazu gehören Viren, Trojaner, Würmer, Spyware, Adware und andere Bedrohungen.

E-Mail-Schutz deaktivieren

Wenn Sie den E-Mail-Schutz deaktivieren, werden potenzielle Bedrohungen in eingehenden (POP3) und ausgehenden (SMTP) E-Mail-Nachrichten und Anhängen nicht erkannt.

So deaktivieren Sie den E-Mail-Schutz:

1. Klicken Sie im Menü "Erweitert" auf **Konfigurieren**.
2. Klicken Sie im Fenster "Konfigurieren" auf **E-Mail & IM**.
3. Klicken Sie unter **E-Mail-Schutz** auf **Aus**.

E-Mail-Schutz aktivieren

Der E-Mail-Schutz erkennt Bedrohungen in eingehenden (POP3) und ausgehenden (SMTP) E-Mail-Nachrichten und Anhängen.

So aktivieren Sie den E-Mail-Schutz:

1. Klicken Sie im Menü "Erweitert" auf **Konfigurieren**.
2. Klicken Sie im Fenster "Konfigurieren" auf **E-Mail & IM**.
3. Klicken Sie unter **E-Mail-Schutz** auf **Ein**.

E-Mail-Schutz konfigurieren

Mit Hilfe der Optionen für den E-Mail-Schutz können sie ein- und ausgehende Nachrichten und Würmer prüfen. Würmer replizieren und verbrauchen Systemressourcen, wodurch die Leistung reduziert bzw. Tasks verlangsamt werden. Würmer können Kopien von sich selbst über E-Mail-Nachrichten verbreiten. Sie können beispielsweise versuchen, E-Mail-Nachrichten an Personen in Ihrem Adressbuch weiterzuleiten.

E-Mail-Schutz konfigurieren

Mit Hilfe der Optionen für den E-Mail-Schutz können sie ein- und ausgehende Nachrichten und Würmer prüfen.

So konfigurieren Sie den E-Mail-Schutz:

1. Klicken Sie im Menü "Erweitert" auf **Konfigurieren**.
2. Klicken Sie im Fenster "Konfigurieren" auf **E-Mail & IM**.
3. Klicken Sie unter **E-Mail-Schutz** auf **Erweitert**.
4. Aktivieren oder deaktivieren Sie die folgenden Kontrollkästchen:
   - **Eingehende E-Mail-Nachrichten überprüfen** Eingehende (POP3) Nachrichten werden auf potenzielle Bedrohungen geprüft.
   - **Ausgehende E-Mail-Nachrichten überprüfen**: Ausgehende (SMTP) Nachrichten werden auf potenzielle Bedrohungen geprüft.
   - **WormStopper aktivieren**: WormStopper blockiert Würmer in E-Mail-Nachrichten.
5. Klicken Sie auf **OK**.

Verwenden des Instant Messaging-Schutzes

Der Instant Messaging-Schutz erkennt Bedrohungen in Anhängen von eingehenden Instant Messaging-Nachrichten.

Instant Messaging-Schutz deaktivieren

Wenn Sie den Instant Messaging-Schutz deaktivieren, werden Bedrohungen in Anhängen von eingehenden Instant Messaging-Nachrichten nicht erkannt.

So deaktivieren Sie den Instant Messaging-Schutz:

1. Klicken Sie im Menü "Erweitert" auf **Konfigurieren**.
2. Klicken Sie im Fenster "Konfigurieren" auf **E-Mail & IM**.
3. Klicken Sie unter **Instant Messaging-Schutz** auf **Aus**.

Instant Messaging-Schutz aktivieren

Der Instant Messaging-Schutz erkennt Bedrohungen in Anhängen von eingehenden Instant Messaging-Nachrichten.

So aktivieren Sie den Instant Messaging-Schutz:

1. Klicken Sie im Menü "Erweitert" auf **Konfigurieren**.
2. Klicken Sie im Fenster "Konfigurieren" auf **E-Mail & IM**.
3. Klicken Sie unter **Instant Messaging-Schutz** auf **Ein**.

KAPITEL 15

Manuelles Prüfen des Computers

Sie können Festplatten, Disketten sowie einzelne Dateien und Ordner nach Viren und anderen Bedrohungen durchsuchen. Wenn VirusScan eine verdächtige Datei findet, versucht es automatisch, die Datei zu bereinigen, sofern es sich dabei nicht um ein potenziell unerwünschtes Programm handelt. Wenn VirusScan die Datei nicht bereinigen kann, können Sie die Datei isolieren oder löschen.

In diesem Kapitel

Manuelles Scannen 102

Manuelles Scannen

Sie können die Überprüfung jederzeit manuell ausführen. Wenn Sie VirusScan beispielsweise gerade installiert haben, können Sie eine Überprüfung ausführen, um sicherzustellen, dass auf Ihrem Computer keine Viren oder andere Bedrohungen vorhanden sind. Wenn Sie die Echtzeit-Überprüfung deaktiviert haben, können Sie eine Überprüfung durchführen, um sicherzustellen, dass Ihr Computer noch sicher ist.

Überpüfung unter Verwendung der Einstellungen für das manuelle Prüfen

Bei diesem Scantyp werden die von Ihnen festgelegten Einstellungen für die manuelle Prüfung verwendet. VirusScan prüft den Inhalt komprimierter Dateien (.zip, .cab usw.), zählt eine komprimierte Datei jedoch als eine Datei. Die Anzahl der durchsuchten Dateien kann auch variieren, wenn Sie seit der letzten Überprüfung Ihre temporären Internetdateien gelöscht haben.

So führen Sie die Überpüfung unter Verwendung der Einstellungen für das manuelle Prüfen aus:

1. Klicken Sie im Menü "Grundlagen" auf **Scannen**. Wenn das Scannen abgeschlossen ist, werden in einer Zusammenfassung die Anzahl der geprüften und erkannten Elemente sowie der Zeitpunkt der letzten Prüfung angezeigt.
2. Klicken Sie auf **Fertig stellen**.

Verwandte Themen

- Konfigurieren manueller Prüfungen (Seite 104)

Scan ohne Verwendung Ihrer Einstellungen für manuelle Scans

Dieser Scan verwendet nicht die von Ihnen festgelegten Einstellungen für manuelle Scans. VirusScan scannt den Inhalt komprimierter Dateien (.zip, .cab etc.), und zählt dabei eine komprimierte Datei als eine Datei. Die Anzahl der durchsuchten Dateien kann auch variieren, wenn Sie seit der letzten Überprüfung Ihre temporären Internetdateien gelöscht haben.

So führen Sie einen Scan ohne Verwendung Ihrer Einstellungen für manuelle Scans durch:

1. Klicken Sie im Menü "Erweitert" auf **Home**.
2. Klicken Sie im Home-Bereich auf **Prüfen**.
3. Aktivieren Sie unter **Zu scannende Bereiche** die Kontrollkästchen neben den Dateien, Ordnern und Laufwerken, die gescannt werden sollen.
4. Aktivieren Sie unter **Optionen** die Kontrollkästchen neben den Dateitypen, die gescannt werden sollen.
5. Klicken Sie auf **Jetzt scannen**. Wenn der Scan beendet ist, wird eine Zusammenfassung angezeigt, in der die Anzahl der gescannten und erkannten Elemente sowie die Anzahl der gesäuberten Elemente und das Datum des letzten Scan angezeigt werden.
6. Klicken Sie auf **Fertig stellen**.

Hinweis: Diese Optionen werden nicht gespeichert.

Scannen in Windows Explorer

Sie können ausgewählte Dateien, Ordner oder Laufwerke in Windows Explorer auf Viren und andere Bedrohungen hin überprüfen.

So durchsuchen Sie Dateien im Windows Explorer:

1. Öffnen Sie Windows Explorer.
2. Klicken Sie mit der rechten Maustaste auf das Laufwerk, den Ordner oder die Datei, die überprüft werden soll, und klicken Sie dann auf **Scannen**. Zur Gewährleistung einer umfassenden Prüfung sind alle Standard-Prüfoptionen ausgewählt.

Konfigurieren manueller Prüfungen

Bei der manuellen oder geplanten Prüfung können Sie die zu prüfenden Dateitypen, die zu prüfenden Speicherorte und den Zeitpunkt der Prüfungen festlegen.

Konfigurieren der zu prüfenden Dateitypen

Sie können die zu prüfenden Dateitypen konfigurieren.

So konfigurieren Sie die zu prüfenden Dateitypen:

1. Klicken Sie im Menü "Erweitert" auf **Konfigurieren**.
2. Klicken Sie im Fenster "Konfigurieren" auf **Computer & Dateien**.
3. Klicken Sie unter **Virenschutz** auf **Erweitert**.
4. Klicken Sie im Fenster "Virenschutz" auf **Manueller Scan**.
5. Aktivieren oder deaktivieren Sie die folgenden Kontrollkästchen:
   - **Mithilfe der Heuristik auf unbekannte Viren prüfen**: Die Dateien werden mit Signaturen bekannter Viren verglichen, um Hinweise auf nicht identifizierte Viren zu erkennen. Diese Option bietet die gründlichste Überprüfung, ist aber meist zeitaufwendiger als eine normale Überprüfung.
   - **ZIP-Dateien und anderen Archivdateien prüfen**: Erkennt und entfernt Viren in .zip- und anderen Archivdateien. Manchmal werden Viren in eine ZIP-Datei eingesetzt und diese ZIP-Datei anschließend in eine andere ZIP-Datei eingefügt, um Anti-Virus-Scanner zu umgehen.
   - **Auf Spyware und potenziell unerwünschte Programme prüfen**: Spyware, Adware und andere Programme, die Ihre Daten ohne Ihre Zustimmung sammeln und weiterleiten, werden erkannt und entfernt.
   - **Nachverfolgungs-Cookies suchen und entfernen**: Cookies, die Ihre Daten ohne Ihre Zustimmung sammeln und weiterleiten, werden erkannt und entfernt. Ein Cookie identifiziert Benutzer, wenn diese eine Webseite besuchen.
   - **Auf Rootkits und andere Stealth-Programme prüfen**: Erkennt und entfernt alle Rootkit- und andere Programme, die sich vor Windows verbergen.
6. Klicken Sie auf eine der folgenden Schaltflächen:
   - **Alle Dateien (empfohlen)**: Jeder aus dem Computer verwendete Dateityp wird geprüft. Mit dieser Option erhalten Sie die gründlichste Überprüfung.
   - **Nur Programmdateien und Dokumente**: Es werden nur Programmdateien und Dokumente geprüft.

7 Klicken Sie auf **OK**.

Konfigurieren der zu prüfenden Speicherorte

Sie können die zu prüfenden Speicherorte für manuelle oder geplante Prüfungen konfigurieren.

So konfigurieren Sie den zu prüfenden Speicherort:

1 Klicken Sie im Menü "Erweitert" auf **Konfigurieren**.

2 Klicken Sie im Fenster "Konfigurieren" auf **Computer & Dateien**.

3 Klicken Sie unter **Virenschutz** auf **Erweitert**.

4 Klicken Sie im Fenster "Virenschutz" auf **Manueller Scan**.

5 Wählen Sie unter **Zu prüfender Standard-Speicherort** die zu prüfenden Dateien, Ordner und Laufwerke aus.

Um eine möglichst umfassende Prüfung zu gewährleisten, wählen Sie die Option **Kritische Dateien**.

6 Klicken Sie auf **OK**.

Planen von Prüfungen

Sie können Prüfungen planen, um Ihren Computer zu festgelegten Intervallen umfassend auf Viren und andere Bedrohungen zu prüfen.

So planen Sie eine Prüfung:

1 Klicken Sie im Menü "Erweitert" auf **Konfigurieren**.

2 Klicken Sie im Fenster "Konfigurieren" auf **Computer & Dateien**.

3 Klicken Sie unter **Virenschutz** auf **Erweitert**.

4 Klicken Sie im Fenster "Virenschutz" auf **Geplanter Scan**.

5 Stellen Sie sicher, dass **Planmäßige Überprüfung aktivieren** ausgewählt ist.

6 Aktivieren Sie das Kontrollkästchen neben dem Wochentag, an dem die Prüfung ausgeführt werden soll.

7 Klicken Sie zum Angeben einer Startzeit in der Liste der Startzeiten auf einen Wert.

8 Klicken Sie auf **OK**.

Tipp: Um den Standardzeitplan zu verwenden, klicken Sie auf **Zurücksetzen.**

KAPITEL 16

Verwalten von VirusScan

Sie können Elemente aus den Listen mit vertrauenswürdigen Elementen löschen, unter Quarantäne gestellte Programme, Cookies und Dateien verwalten, Ereignisse und Protokolle anzeigen und McAfee verdächtige Aktivitäten melden.

In diesem Kapitel

Verwalten vertrauenswürdiger Listen 108
Verw. isolierter Programme, Cookies und Dateien ..109
Anzeigen zuletzt aufg. Ereignisse und Protokolle.....111
Autom. Melden anonymer Informationen.....112
Grundlegendes zu Sicherheitswarnungen 113

Verwalten vertrauenswürdiger Listen

Wenn Sie einem SystemGuard, Programm, Pufferüberlauf oder E-Mail-Programm vertrauen, wird das Element einer Liste vertrauenswürdiger Elemente hinzugefügt, so dass das Element nicht mehr erkannt wird.

Wenn Sie einem Programm versehentlich vertrauen oder wenn ein Programm erkannt werden soll, müssen Sie es aus dieser Liste entfernen.

Verwalten vertrauenswürdiger Listen

Wenn Sie einem SystemGuard, Programm, Pufferüberlauf oder E-Mail-Programm vertrauen, wird das Element einer Liste vertrauenswürdiger Elemente hinzugefügt, so dass das Element nicht mehr erkannt wird.

Wenn Sie einem Programm versehentlich vertrauen oder wenn ein Programm erkannt werden soll, müssen Sie es aus dieser Liste entfernen.

So entfernen Sie Elemente aus den Listen mit vertrauenswürdigen Elementen:

1. Klicken Sie im Menü "Erweitert" auf **Konfigurieren**.
2. Klicken Sie im Fenster "Konfigurieren" auf **Computer & Dateien**.
3. Klicken Sie unter **Virenschutz** auf **Erweitert**.
4. Klicken Sie im Fenster "Virenschutz" auf **Listen mit vertrauenswürdigen Elementen**.
5. Wählen Sie in der Liste ein vertrauenswürdiges Objekt des Typs SystemGuard, Programm, Pufferüberlauf oder E-Mail-Programm aus, um dessen Elemente und ihren Vertrauensstatus anzuzeigen.
6. Unter **Details** finden Sie Informationen zu diesem Element.
7. Klicken Sie unter **Ich möchte** auf eine Aktion.
8. Klicken Sie auf **OK**.

Verw. isolierter Programme, Cookies und Dateien

Unter Quarantäne gestellte Programme, Cookies und Dateien können wiederhergestellt, gelöscht oder zur Analyse an McAfee gesendet werden.

Wiederherstellen von unter Quarantäne gestellten Programmen, Cookies und Dateien

Falls erforderlich, können Sie Programme, Cookies und Dateien, die unter Quarantäne gestellt wurden, wiederherstellen.

So stellen Sie unter Quarantäne gestellte Programme, Cookies und Dateien wieder her:

1. Klicken Sie im Menü "Erweitert" auf **Wiederherstellen**.
2. Klicken Sie im Fenster "Wiederherstellen" auf **Programme und Cookies** oder **Dateien**.
3. Wählen Sie die unter Quarantäne gestellten Programme, Cookies oder Dateien aus, die wiederhergestellt werden sollen.
4. Weitere Informationen zu einem unter Quarantäne gestellten Virus erhalten Sie, wenn Sie unter **Details** auf seinen Erkennungsnamen klicken. Zusammen mit der Virenbeschreibung wird die Virenbibliothek angezeigt.
5. Klicken Sie unter **Ich möchte** auf **Wiederherstellen**.

Entfernen von unter Quarantäne gestellten Programmen, Cookies und Dateien

Sie können unter Quarantäne gestellte Programme, Cookies und Dateien entfernen.

So entfernen Sie unter Quarantäne gestellte Programme, Cookies und Dateien:

1. Klicken Sie im Menü "Erweitert" auf **Wiederherstellen**.
2. Klicken Sie im Fenster "Wiederherstellen" auf **Programme und Cookies** oder **Dateien**.
3. Wählen Sie die unter Quarantäne gestellten Programme, Cookies oder Dateien aus, die wiederhergestellt werden sollen.
4. Weitere Informationen zu einem unter Quarantäne gestellten Virus erhalten Sie, wenn Sie unter **Details** auf seinen Erkennungsnamen klicken. Zusammen mit der Virenbeschreibung wird die Virenbibliothek angezeigt.
5. Klicken Sie unter **Ich möchte** auf **Entfernen**.

Unter Quarantäne gestellte Programme, Cookies und Dateien an McAfee senden

Sie können unter Quarantäne gestellte Programme, Cookies und Dateien zur Analyse an McAfee senden.

Hinweis: Wenn die unter Quarantäne gestellte Datei, die Sie senden möchten, die maximal zulässige Größe überschreitet, kann die Datei abgelehnt werden. In den meisten Fällen ist dies jedoch nicht der Fall.

So senden Sie unter Quarantäne gestellte Programme oder Dateien an McAfee:

1. Klicken Sie im Menü "Erweitert" auf **Wiederherstellen**.
2. Klicken Sie im Fenster "Wiederherstellen" auf **Programme und Cookies** oder **Dateien**.
3. Wählen Sie die unter Quarantäne gestellten Programme, Cookies oder Dateien aus, die an McAfee gesendet werden sollen.
4. Weitere Informationen zu einem unter Quarantäne gestellten Virus erhalten Sie, wenn Sie unter **Details** auf seinen Erkennungsnamen klicken. Zusammen mit der Virenbeschreibung wird die Virenbibliothek angezeigt.
5. Klicken Sie unter **Ich möchte** auf **An McAfee senden**.

Anzeigen zuletzt aufg. Ereignisse und Protokolle

Unter "Zuletzt aufgetretene Ereignisse" und "Protokolle" werden Ereignisse zu allen installierten McAfee-Produkten angezeigt.

Unter "Zuletzt aufgetretene Ereignisse" können Sie die letzten 30 signifikanten Ereignisse sehen, die auf Ihrem Computer aufgetreten sind. Sie können blockierte Programme wiederherstellen, die Echtzeitprüfung neu aktivieren und Pufferüberläufen vertrauen.

Außerdem können sie Protokolle anzeigen, in denen alle Ereignisse der letzten 30 Tage aufgezeichnet werden.

Ereignisse anzeigen

Unter "Zuletzt aufgetretene Ereignisse" können Sie die letzten 30 signifikanten Ereignisse sehen, die auf Ihrem Computer aufgetreten sind. Sie können blockierte Programme wiederherstellen, die Echtzeitprüfung neu aktivieren und Pufferüberläufen vertrauen.

So zeigen Sie Ereignisse an:

1. Klicken Sie im Menü "Erweitert" auf **Berichte & Protokolle**.
2. Klicken Sie im Fenster "Berichte & Protokolle" auf **Zuletzt aufgetretene Ereignisse**.
3. Wählen Sie das Ereignis aus, das Sie sich ansehen möchten.
4. Unter **Details** finden Sie Informationen zu diesem Ereignis.
5. Klicken Sie unter **Ich möchte** auf eine Aktion.

Protokolle anzeigen

In Protokollen werden alle Ereignisse aufgezeichnet, die in den letzten 30 Tagen aufgetreten sind.

So zeigen Sie Protokolle an:

1. Klicken Sie im Menü "Erweitert" auf **Berichte & Protokolle**.
2. Klicken Sie im Fenster "Berichte & Protokolle" auf **Zuletzt aufgetretene Ereignisse**.
3. Klicken Sie im Fenster "Zuletzt aufgetretene Ereignisse" auf **Protokoll anzeigen**.
4. Wählen Sie den Protokoll aus, den Sie sich ansehen möchten, und wählen Sie anschließend ein Protokoll aus.
5. Unter **Details** finden Sie Informationen zu diesem Protokoll.

Autom. Melden anonymer Informationen

Sie können Viren, potenziell unerwünschte Programme und Hacker-Informationen anonym an McAfee senden. Diese Option ist nur während der Installation verfügbar.

Es werden keine Informationen gesammelt, anhand derer Sie persönlich identifiziert werden können.

Bei McAfee melden

Sie können Viren, potenziell unerwünschte Programme und Hacker-Informationen an McAfee senden. Diese Option ist nur während der Installation verfügbar.

So melden Sie anonyme Informationen automatisch:

1. Übernehmen Sie bei der Installation von VirusScan die Vorgabe **Anonyme Informationen übermittteln**.
2. Klicken Sie auf **Weiter**.

Grundlegendes zu Sicherheitswarnungen

Wenn die Echtzeitprüfung eine Bedrohung erkennt, wird eine Warnung angezeigt. Bei den meisten Viren, Trojanern und Würmern versucht die Echtzeitprüfung automatisch, die Datei zu bereinigen, und zeigt eine Warnung an. Bei potenziell unerwünschten Programmen und SystemGuards wird die Datei oder Änderung von der Echtzeitprüfung ermittelt, automatisch blockiert und eine Warnung angezeigt. Bei Pufferüberlauf, Nachverfolgungs-Cookies und Skriptaktivitäten blockiert die Echtzeitprüfung die Aktivität automatisch und benachrichtigt Sie.

Diese Warnungen können in drei Grundarten eingeteilt werden.

- Rote Warnungen
- Gelbe Warnungen
- Grüne Warnungen

Sie können anschließend festlegen, wie mit erkannten Dateien, E-Mails, verdächtigen Skripts, potenziellen Würmern, potenziell unerwünschten Programmen, SystemGuards oder Pufferüberläufen verfahren werden soll.

Verwalten von Warnungen

McAfee bietet mehrere Warnungen, um Sie bei der Verwaltung der Sicherheit zu unterstützen. Diese Warnungen können in drei Grundarten eingeteilt werden.

- Rote Warnungen
- Gelbe Warnungen
- Grüne Warnungen

Rote Warnungen

Bei einer roten Warnung ist ein Eingreifen Ihrerseits erforderlich. In einigen Fällen kann McAfee nicht ermitteln, wie es automatisch auf eine bestimmte Aktivität reagieren soll. In diesen Fällen wird die entsprechende Aktivität in einer roten Warnung beschrieben und Sie haben mehrere Optionen zur Auswahl.

Gelbe Warnungen

Eine gelbe Warnung ist eine nicht-kritische Benachrichtigung, bei der in der Regel kein Eingreifen Ihrerseits erforderlich ist. Die entsprechende Aktivität wird in einer gelben Warnung beschrieben und Sie haben mehrere Optionen zur Auswahl.

Grüne Warnungen

In den meisten Fällen enthalten grüne Warnungen allgemeine Angaben zu einem Ereignis und es ist kein Eingreifen Ihrerseits erforderlich.

Konfigurieren von Warnoptionen

Wenn Sie nicht möchten, dass eine Warnung noch einmal angezeigt wird und dies später ändern möchten, haben Sie die Möglichkeit, dies entsprechend zu konfigurieren. Weitere Informationen zum Konfigurieren von Warnoptionen finden Sie in der SecurityCenter-Dokumentation.

KAPITEL 17

Zusätzliche Hilfe

In diesem Kapitel werden die häufig gestellte Fragen und Fehlerbehebungsszenarios beschrieben.

In diesem Kapitel

Fragen und Antworten (FAQs) 116
Problembehandlung 118

Fragen und Antworten (FAQs)

Dieser Abschnitt enthält Antworten zu den am häufigsten gestellten Fragen.

Eine Bedrohung wurde erkannt. Wie soll ich vorgehen?

McAfee verwendet Warnungen, um Ihre Sicherheit zu verwalten. Diese Warnungen lassen sich in drei allgemeine Typen aufteilen.

- Rote Warnungen
- Gelbe Warnungen
- Grüne Warnungen

Sie können anschließend festlegen, wie erkannte Dateien, entdeckte E-Mails, verdächtige Skripts, potentielle Würmer, potentiell unerwünschte Programme, SystemGuards oder Pufferüberläufe verwaltet werden sollen.

Weitere Informationen zur Verwaltung bestimmter Bedrohungen finden Sie in der Virus-Informationsbibliothek unter: http://us.mcafee.com/virusInfo/default.asp?affid=.

Verwandte Themen

- Grundlegendes zu Sicherheitswarnungen (Seite 113)

Kann ich VirusScan mit den Browsern "Netscape", "Firefox" und "Opera" verwenden?

Sie können Netscape, Firefox oder Opera als Standardbrowser verwenden, müssen jedoch auch Microsoft Internet Explorer ab Version 6.0 auf Ihrem Computer installiert haben.

Ist zur Ausführung einer Prüfung eine Internetverbindung erforderlich?

Zum Ausführen einer Prüfung müssen Sie nicht mit dem Internet verbunden sein. Sie sollten aber mindestens einmal wöchentlich eine Verbindung zum Internet herstellen, damit McAfee-Aktualisierungen empfangen werden können.

Überprüft VirusScan E-Mail-Anlagen?

Wenn Sie die Echtzeitprüfung und den E-Mail-Schutz aktiviert haben, werden beim Eingang der E-Mail-Nachricht alle Anhänge geprüft.

Überprüft VirusScan auch komprimierte Dateien?

VirusScan prüft .ZIP-Dateien und andere Archivdateien.

Warum treten bei der Prüfung ausgehender E-Mails Fehler auf?

Bei der Prüfung ausgehender E-Mail-Nachrichten können folgende Fehlertypen auftreten:

- Protokollfehler. Der E-Mail-Server hat eine E-Mail-Nachricht abgelehnt.
  Wenn ein Protokoll- oder Systemfehler auftritt, werden die verbleibenden E-Mail-Nachrichten für die entsprechende Sitzung weiter verarbeitet und an den Server gesendet.
- Verbindungsfehler. Eine Verbindung zum E-Mail-Server wurde abgebrochen.
  Wenn ein Verbindungsfehler auftritt, vergewissern Sie sich, dass Ihr Computer mit dem Internet verbunden ist, und versuchen Sie, die Nachricht über die Liste der **gesendeten** Nachrichten Ihres E-Mail-Programms erneut zu senden.
- Systemfehler. Es ist ein Filehandling- bzw. ein anderer Systemfehler aufgetreten.
- Fehler mit verschlüsselter SMTP-Verbindung. Es wurde eine verschlüsselte SMTP-Verbindung mit Ihrem E-Mail-Programm festgestellt.
  Wenn ein Fehler mit der verschlüsselten SMTP-Verbindung auftritt, deaktivieren Sie die verschlüsselte SMTP-Verbindung in Ihrem E-Mail-Programm, um sicherzustellen, dass Ihre E-Mail-Nachrichten überprüft werden.

Wenn beim Senden von E-Mail-Nachrichten Zeitüberschreitungen auftreten, deaktivieren Sie die Überprüfung ausgehender E-Mail-Nachrichten oder deaktivieren Sie die verschlüsselte SMTP-Verbindung in Ihrem E-Mail-Programm.

Verwandte Themen

- E-Mail-Schutz konfigurieren (Seite 99)

Problembehandlung

Dieser Abschnitt enthält Hilfe zu allgemeinen Problemen, die auftreten können.

Ein Virus kann nicht bereinigt oder gelöscht werden

Einige Viren müssen Sie manuell vom Computer entfernen. Versuchen Sie, Ihren Computer neu zu starten und die Prüfung erneut auszuführen.

Wenn der Computer einen Virus nicht selbständig bereinigen oder löschen kann, verwenden Sie die Virus Information Library unter: http://us.mcafee.com/virusInfo/default.asp?affid=.

Weitere Unterstützung erhalten Sie vom McAfee-Kundendienst auf der McAfee-Website.

Hinweis: Viren können nicht von CD-ROMs, DVDs oder schreibgeschützten Disketten entfernt werden.

Ein Element kann auch nach dem Neustart nicht entfernt werden

In einigen Fällen ist es erforderlich, dass Sie Ihren Computer nach dem Prüfen und Entfernen von Elementen neu starten.

Wenn das Element nach dem Neustart des Computers nicht entfernt werden kann, senden Sie die Datei an McAfee.

Hinweis: Viren können nicht von CD-ROMs, DVDs oder schreibgeschützten Disketten entfernt werden.

Verwandte Themen

- Verwalten von unter Quarantäne gestellten Programmen, Cookies und Dateien (Seite 109)

Komponenten fehlen oder sind beschädigt

Einige Situationen können zu einer fehlerhaften Installation von VirusScan führen:

- Es ist nicht genügend Festplattenplatz oder Arbeitsspeicher auf Ihrem Computer verfügbar. Stellen Sie sicher, dass Ihr Computer den Systemanforderungen der Software entspricht.
- Der Internetbrowser ist nicht richtig konfiguriert.
- Ihre Internetverbindung ist fehlerhaft. Überprüfen Sie Ihre Verbindung oder versuchen Sie später noch einmal, eine Verbindung herzustellen.
- Dateien fehlen oder die Installation schlägt fehl.

Versuchen Sie, potenzielle Probleme zu beheben, und installieren Sie VirusScan anschließend erneut.

KAPITEL 18

McAfee Personal Firewall

Personal Firewall bietet erweiterten Schutz für Ihren Computer und Ihre persönlichen Daten. Personal Firewall errichtet eine Barriere zwischen Ihrem Computer und dem Internet. Dabei wird der Internetverkehr im Hintergrund auf verdächtige Aktivitäten überwacht.

In diesem Kapitel

Funktionen 122
Firewall starten 125
Mit Warnungen arbeiten 127
Informationswarnungen verwalten 131
Firewall-Schutz konfigurieren 133
Programme und Berechtigungen verwalten 147
Systemdienste verwalten 161
Computerverbindungen verwalten 167
Protokollierung, Überwachung und Analyse 179
Weitere Informationen zu Internet Security 195

Funktionen

Personal Firewall bietet Schutz bei ein- und ausgehenden Verbindungen, vertraut automatisch bekannten gutartigen Programmen und hilft dabei, Spyware, Trojaner und Keylogger-Programme zu blockieren. Mit Firewall können Sie Hacker-Angriffe abwehren, die Internet- und Netzwerkaktivität überwachen, sich über feindliche oder verdächtige Ereignisse benachrichtigen lassen, detaillierte Informationen zum Internetverkehr anzeigen und Antivirus-Abwehrstrategien ergänzen.

Standardmäßige und benutzerdefinierte Sicherheitsstufen

Schützen Sie sich mit Hilfe der standardmäßigen Einstellungen von Firewall vor Intrusion-Angriffen und verdächtigen Aktivitäten oder passen Sie Firewall an Ihre Sicherheitsanforderungen an.

Empfehlungen in Echtzeit

Lassen Sie sich dynamisch Empfehlungen zukommen, um zu ermitteln, ob Programmen Internetzugriff gewährt werden oder Netzwerkverkehr als vertrauenswürdig eingestuft werden soll.

Intelligente Zugriffsverwaltung für Programme

Im Firewall-Fenster "Programmberechtigungen" verwalten Sie den Internetzugriff für Programme über Warnungen und Ereignisprotokolle oder Sie konfigurieren Zugriffsberechtigungen für bestimmte Programme.

Gaming-Schutz

Sie können verhindern, dass Warnungen zu Einbruchsversuchen und verdächtigen Aktivitäten während des Spielens im Vollbildmodus angezeigt werden, und Firewall so konfigurieren, dass die Warnungen nach Abschluss des Computerspiels angezeigt werden.

Schutz beim Computer-Start

Bevor Windows gestartet wird, schützt Firewall Ihren Computer vor Einbruchsversuchen sowie vor unerwünschten Programmen und unerwünschtem Netzwerkverkehr.

Kontrolle des Systemdienstanschlusses

Systemdienstanschlüsse können ein Sicherheitsrisiko für Ihren Computer darstellen. Mit Firewall können Sie die für einige Programme erforderlichen offenen und geschlossenen Systemdienstanschlüsse erstellen und verwalten.

Verwalten von Computer-Verbindungen

Sie können Remote-Verbindungen und IP-Adressen, die eine Verbindung zu Ihrem Computer herstellen, als vertrauenswürdig einstufen oder blockieren.

Integration von HackerWatch-Informationen

HackerWatch ist ein Sicherheitsinformations-Hub, der globale Hacking- und Intrusion-Muster verfolgt und die aktuellsten Informationen zu Programmen auf Ihrem Computer zur Verfügung stellt. Außerdem haben Sie die Möglichkeit, globale Sicherheitsereignisse und Statistiken zu Internetanschlüssen anzuzeigen.

Firewall sperren

Des Weiteren können Sie den gesamten ein- und ausgehenden Netzwerkverkehr zwischen Ihrem Computer und dem Internet sofort sperren.

Sicherheitseinstellungen für Firewall wiederherstellen

Sie können die ursprünglichen Sicherheitseinstellungen für Firewall wiederherstellen. Wenn sich Personal Firewall nicht so verhält, wie Sie es wünschen, haben Sie die Möglichkeit, Ihre aktuellen Einstellungen rückgängig zu machen und die Standardeinstellungen des Produkts wiederherzustellen.

Erweiterte Erkennung von Trojanern

Personal Firewall verwaltet Programmverbindungen mit einer erweiterten Datenbank, mit der mehr potenziell bösartige Anwendungen, beispielsweise Trojaner, erkannt und blockiert und somit daran gehindert werden können, auf das Internet zuzugreifen und möglicherweise Ihre persönlichen Daten weiterzugeben.

Ereignisprotokollierung

Legen Sie fest, ob die Protokollierung aktiviert oder deaktiviert werden soll, und, wenn sie aktiviert wird, welche Ereignistypen protokolliert werden sollen. Mit der Ereignisprotokollierung können Sie zuletzt aufgetretende ein- oder ausgehende Ereignisse anzeigen. Außerdem haben Sie die Möglichkeit, Ereignisse anzuzeigen, die auf Einbruchsversuche hindeuten.

Überwachen des Internetverkehrs

Sie können einfach zu lesende grafische Karten prüfen, auf der die Quelle von feindlichen Angriffen und Datenverkehr weltweit angezeigt werden. Zudem werden detaillierte Eigentümerinformationen und geografische Daten für Ursprungs-IP-Adressen bereitgestellt. Des Weiteren können Sie ein- und ausgehenden Verkehr analysieren sowie die Programmbandbreite und die Programmaktivität überwachen.

Eindringschutz

Schützt Ihre Privatsphäre, indem Eindringschutz gegen mögliche Bedrohungen aus dem Internet zur Verfügung gestellt wird. Durch die Verwendung Heuristik-ähnlicher Funktionen bietet McAfee eine dritte Schutzstufe, da alle Objekte blockiert werden, die Angriffssymptome oder Eigenschaften von Hacker-Angriffen aufweisen.

Intelligente Datenverkehrsanalyse

Prüft sowohl ein- als auch ausgehenden Internetverkehr und Programmverbindungen, einschließlich derer, die aktiv offene Verbindungen überwachen. Dies ermöglicht Ihnen, Programme zu erkennen, die möglicherweise ein Risiko darstellen, und entsprechende Gegenmaßnahmen zu treffen.

Firewall starten

Schon direkt nach der Installation von Firewall ist Ihr Computer vor Intrusionsversuchen und unerwünschtem Internetdatenverkehr geschützt. Darüber hinaus können Sie mit Firewall Warnungen erhalten sowie den Zugriff auf eingehende und ausgehende Internetverbindungen bekannter und unbekannter Programme verwalten. Empfehlungen und Standardsicherheit sind automatisch aktiviert.

Sie können Firewall zwar im Bereich "Internet & Netzwerkkonfiguration" deaktivieren, jedoch ist Ihr Computer dann nicht mehr gegen Intrusionsversuche und unerwünschten Internetdatenverkehr geschützt. Außerdem sind Sie dann nicht mehr in der Lage, eingehende und ausgehende Internetverbindungen effektiv zu verwalten. Daher sollten Sie den Firewall-Schutz nur vorübergehend und nur wenn absolut notwendig deaktivieren. Sie können Firewall auch im Bereich "Internet & Netzwerkkonfiguration" aktivieren.

Firewall deaktiviert automatisch die Windows® Firewall und richtet sich selbsttätig als standardmäßige Firewall ein.

Hinweis: Öffnen Sie zum Konfigurieren von Firewall das Fenster "Netzwerk- & Internetkonfiguration".

Firewall-Schutz aktivieren

Das Aktivieren der Firewall schützt Ihren Computer vor Intrusionsversuchen und unerwünschtem Internetdatenverkehr. Damit können außerdem eingehende und ausgehende Internetverbindungen verwaltet werden.

So aktivieren Sie den Firewall-Schutz:

1. Führen Sie im Bereich "McAfee SecurityCenter" einen der folgenden Schritte aus:
   - Wählen Sie **Internet & Netzwerk**, und klicken Sie dann auf **Konfigurieren**.
   - Wählen Sie das Menü **Erweitert** und dann im Bereich **Startseite** die Option **Konfigurieren**. Zeigen Sie auf **Internet & Netzwerk**.
2. Klicken Sie im Bereich **Internet & Netzwerkkonfiguration** unter **Firewall-Schutz** auf **Ein**.

Firewall-Schutz deaktivieren

Durch das Deaktivieren des Firewall-Schutzes wird Ihr Computer anfällig gegenüber Intrusionsversuchen und unerwünschtem Internetdatenverkehr. Außerdem können Sie ohne den Firewall-Schutz keine eingehenden und ausgehenden Internetverbindungen verwalten.

So deaktivieren Sie den Firewall-Schutz:

1. Führen Sie im Bereich "McAfee SecurityCenter" einen der folgenden Schritte aus:
   - Wählen Sie **Internet & Netzwerk**, und klicken Sie dann auf **Konfigurieren**.
   - Wählen Sie das Menü **Erweitert** und dann im Bereich **Startseite** die Option **Konfigurieren**. Zeigen Sie auf **Internet & Netzwerk**.
2. Klicken Sie im Bereich **Internet & Netzwerkkonfiguration** unter **Firewall-Schutz** auf **Aus**.

Mit Warnungen arbeiten

Firewall unterstützt Sie mit verschiedenen Warnungen bei der Verwaltung Ihrer Sicherheit. Diese Warnungen lassen sich in vier allgemeine Typen aufteilen.

- Warnung "Trojaner blockiert"
- Rote Warnungen
- Gelbe Warnungen
- Grüne Warnungen

Warnungen können auch Empfehlungen enthalten, wie Benutzer bei angezeigten Warnungen vorgehen sollten. In anderen Warnungen werden Benutzer darauf hingewiesen, wie Sie weitere Informationen zu den auf Ihrem Computer ausgeführten Programmen erhalten können.

Allgemeines zu Warnungen

Firewall verfügt über vier allgemeine Warnungstypen. Einige Warnungen enthalten Hinweise, wie sie weitere Informationen zu den auf Ihrem Computer ausgeführten Programmen erhalten können.

Warnung "Trojaner blockiert"

Trojaner tarnen sich als legale Programme und können zu Schäden an Ihrem Computer sowie zu Systemabstürzen führen. Außerdem können sie Unbefugten Zugriff auf Ihren Computer gewähren. Die Warnung "Trojaner blockiert" wird angezeigt, wenn Firewall einen Trojaner auf Ihrem Computer erkennt und dann blockiert. Sie sollten Ihr System in jedem Fall nach weiteren Bedrohungen scannen. Diese Warnung wird bei jeder Sicherheitsstufe angezeigt, außer bei der Sicherheitsstufe "Offen" oder wenn die Option "Empfehlungen" deaktiviert ist.

Rote Warnungen

Der häufigste Warnungstyp ist die rote Warnung. Er erfordert im Allgemeinen ein Eingreifen durch den Benutzer. Da Firewall in einigen Fällen die notwendigen Aktionen für eine Programmaktivität bzw. ein Netzwerkereignis nicht automatisch feststellen kann, beschreibt die Warnung zunächst die aktuelle Programmaktivität (bzw. das Netzwerkereignis) und führt dann eine oder mehrere Optionen auf, auf die Sie reagieren müssen. Wenn die Option "Empfehlungen" aktiviert ist, werden Programme zum Bereich "Programmberechtigungen" hinzugefügt.

Folgende Warnmeldungen treten am häufigsten auf:

- **Das Programm fordert Zugriff auf das Internet an**: Firewall hat ein Programm erkannt, das versucht, eine Verbindung zum Internet herzustellen.
- **Das Programm wurde geändert**: Firewall hat eine Änderung an einem Programm erkannt. Dabei kann es sich eventuell um das Ergebnis einer Onlineaktualisierung handeln.
- **Programm blockiert**: Firewall blockiert ein Programm, da es im Bereich "Programmberechtigungen" aufgeführt ist.

In Abhängigkeit Ihrer Einstellungen und der Programmaktivität bzw. des Netzwerkereignisses werden die folgenden Optionen am häufigsten angezeigt:

- **Zugriff gewähren**: Gewährt einem Programm auf Ihrem Computer den Zugriff auf das Internet. Diese Regel wird dem Bereich "Programmberechtigungen" hinzugefügt.
- **Zugriff einmal gewähren**: Gestattet einem Programm auf Ihrem Computer temporären Zugriff auf das Internet. Ein einmaliger Zugriff auf das Internet ist beispielsweise bei der Installation eines neuen Programms erforderlich.
- **Zugriff blockieren**: Verhindert, dass ein bestimmtes Programms auf das Internet zugreift.
- **Nur ausgehenden Zugriff gewähren**: Gestattet einem bestimmten Programm nur den Zugriff auf eine ausgehende Internetverbindung. Diese Warnung wird in der Regel nur dann angezeigt, wenn die Sicherheitsstufen "Eingeschränkt" und "Stealth" eingestellt sind.
- **Diesem Netzwerk vertrauen**: Gestattet eingehenden und ausgehenden Datenverkehr von einem Netzwerk. Das Netzwerk wird dem Bereich "Vertrauenswürdige IP-Adressen" hinzugefügt.
- **Diesem Netzwerk derzeit nicht vertrauen**: Blockiert eingehenden und ausgehenden Datenverkehr von einem Netzwerk.

Gelbe Warnung

Bei gelben Warnungen handelt es sich um nichtkritische Benachrichtigungen, die Sie über von Firewall erkannte Netzwerkereignisse informieren. Beispielsweise wird die Warnung **Neues Netzwerk gefunden** angezeigt, wenn Firewall das erste Mal ausgeführt wird oder wenn ein Computer, auf dem Firewall installiert ist, mit einem neuen Netzwerk verbunden wird. Sie können entscheiden, ob das Netzwerk vertrauenswürdig oder nicht vertrauenswürdig ist. Wenn das Netzwerk vertrauenswürdig ist, gestattet Firewall den Datenverkehr von anderen Computern in diesem Netzwerk, und das Netzwerk wird dem Bereich "Vertrauenswürdige IP-Adressen" hinzugefügt.

Grüne Warnung

In den meisten Fällen enthalten grüne Warnungen allgemeine Informationen zu einem Ereignis. Auf grüne Warnungen muss nicht reagiert werden. Grüne Warnungen treten in der Regel nur dann auf, wenn die Sicherheitsstufen "Standardsicherheit", "Eingeschränkte Sicherheit", "Stealth" und "Verbindung schließen" eingestellt sind. Die folgenden grünen Warnmeldungen sind möglich:

- **Das Programm wurde geändert**: Informiert Sie darüber, dass ein Programm, dem Sie zuvor den Zugriff auf das Internet gestattet hatten, verändert wurde. Sie können das Programm blockieren, wenn Sie jedoch nicht eingreifen, wird die Warnmeldung geschlossen und das Programm hat weiterhin Zugriff auf das Internet.
- **Programm kann auf das Internet zugreifen**: Informiert Sie darüber, dass einem Programm der Zugriff auf das Internet gewährt wurde. Sie können das Programm blockieren, wenn Sie jedoch nicht eingreifen, wird die Warnmeldung geschlossen und das Programm hat weiterhin Zugriff auf das Internet.

Benutzereingriff

Viele Firewall-Warnungen enthalten weiterführende Informationen, die Sie bei der Verwaltung der Sicherheit Ihres Computers unterstützen. Hierzu gehören die folgenden Meldungen:

- **Weitere Informationen über dieses Programm**: Startet die McAfee-Website zur globalen Sicherheit, auf der Sie Informationen zu einem Programm finden, das Firewall auf Ihrem Computer erkannt hat.
- **Informieren Sie McAfee über dieses Programm**: Senden Sie Informationen über eine unbekannte Datei, die Firewall auf Ihrem Computer erkannt hat, an McAfee.
- **McAfee-Empfehlung**: Empfehlungen zur Handhabung von Warnungen. Beispielsweise kann eine Warnung empfehlen, dass Sie einem Programm den Zugriff auf das Internet gewähren.

Informationswarnungen verwalten

Mit Firewall können Sie Informationswarnungen während bestimmter Ereignisse anzeigen oder ausblenden.

Warnungen während eines Spiels anzeigen

In der Standardeinstellung verhindert Firewall, dass Informationswarnungen angezeigt werden, während ein Spiel im Vollbild angezeigt wird. Sie können Firewall jedoch auch so konfigurieren, dass Informationswarnungen während eines Spiels angezeigt werden, wenn Firewall einen Intrusionsversuch oder eine verdächtige Aktivität feststellt.

So zeigen Sie Warnungen während eines Spiels an:

1. Klicken Sie im Fenster "Häufige Tasks" auf das Menü **Erweitert**.
2. Klicken Sie auf **Konfigurieren**.
3. Klicken Sie im Fenster zur SecurityCenter-Konfiguration auf **Warnungen**.
4. Klicken Sie auf **Erweitert**.
5. Aktivieren Sie im Bereich **Warnoptionen** die Option **Informationswarnungen einblenden, wenn Gaming-Modus erkannt wird**.

Informationswarnungen verbergen

Informationswarnungen benachrichtigen Sie bei Ereignissen, die Ihr unmittelbares Eingreifen nicht erforderlich machen.

So verbergen Sie Informationswarnungen:

1. Klicken Sie im Fenster "Häufige Tasks" auf das Menü **Erweitert**.
2. Klicken Sie auf **Konfigurieren**.
3. Klicken Sie im Fenster zur SecurityCenter-Konfiguration auf **Warnungen**.
4. Klicken Sie auf **Erweitert**.
5. Klicken Sie im Bereich **SecurityCenter-Konfiguration** auf die Option **Informationswarnungen**.
6. Führen Sie im Bereich **Informationswarnungen** einen der folgenden Schritte aus:
   - Wählen Sie den zu verbergenden Warnungstyp aus.
   - Wählen Sie **Informationswarnungen verbergen**, um alle Informationswarnungen zu verbergen.
7. Klicken Sie auf **OK**.

KAPITEL 19

Firewall-Schutz konfigurieren

Firewall bietet verschiedene Methoden zur Verwaltung Ihrer Sicherheit und zum Anpassen der Art und Weise, wie auf Sicherheitsereignisse und -warnungen reagiert werden soll.

Nach der Erstinstallation von Firewall wird die Schutzebene auf "Standardsicherheit" gesetzt. In der Regel erfüllt diese Einstellung alle Sicherheitsanforderungen. Dennoch bietet Ihnen Firewall auch andere Sicherheitsstufen an, die von "Verbindung schließen" (sehr restriktiv) bis "Offen" (sehr tolerant) reichen.

Darüber hinaus kann Firewall Empfehlungen bei Warnungen und dem Internetzugriff von Programmen anzeigen.

In diesem Kapitel

Firewall-Sicherheitsstufen verwalten 134
Empfehlungen für Warnungen konfigurieren 138
Firewall-Sicherheit optimieren 140
Firewall sperren und wiederherstellen 144

Firewall-Sicherheitsstufen verwalten

Sie können die Sicherheitsstufen Ihren Anforderungen entsprechend anpassen, so dass Sie beispielsweise nur dann eingreifen müssen, wenn Firewall unerwünschten Netzwerkdatenverkehr sowie eingehende und ausgehende Internetverbindungen erkannt. In der Standardeinstellung ist die Sicherheitsstufe "Standardsicherheit" aktiviert.

Wenn die Sicherheitsstufe "Standardsicherheit" eingestellt und die Option "Empfehlungen" aktiviert ist, können Sie bei roten Warnungen den Zugriff für unbekannte oder geänderte Programme gewähren oder blockieren. Bei bekannten Programmen werden grüne Informationsmeldungen angezeigt und der Zugriff wird automatisch gewährt. Durch das Gewähren des Zugriffs kann eine Anwendung ausgehende Verbindungen herstellen und auf unaufgeforderte eingehende Verbindungen hin überwachen.

Allgemein gilt, je restriktiver eine Sicherheitsstufe ("Stealth" und "Eingeschränkte Sicherheit"), desto größer ist die Anzahl an Optionen und Warnungen, die angezeigt werden und Ihr Eingreifen erforderlich machen.

Firewall bietet sechs Sicherheitsstufen. Beginnend mit der restriktiven zur tolerantesten lauten die Sicherheitsstufen wie folgt:

- **Verbindung schließen**: Blockiert alle Internetverbindungen.
- **Stealth**: Blockiert alle eingehenden Internetverbindungen.
- **Eingeschränkte Sicherheit**: Warnungen erfordern Ihr Eingreifen bei jeder eingehenden und ausgehenden Internetverbindungsanforderung.
- **Standardsicherheit**: Warnungen werden angezeigt, wenn unbekannte oder neue Programme den Internetzugriff anfordern.
- **Vertrauenswürdige Sicherheit**: Gewährt alle eingehenden und ausgehenden Netzwerkverbindungen und fügt diese automatisch dem Bereich "Programmberechtigungen" hinzu.
- **Offen**: Gewährt alle eingehenden und ausgehenden Internetverbindungen.

Im Firewall-Bereich "Standardwerte für Firewall-Schutz wiederherstellen" können Sie Ihre Sicherheitsstufe unmittelbar wieder auf "Standardsicherheit" zurücksetzen.

Die Sicherheitsstufe "Verbindung schließen"

Bei der Firewall-Sicherheitsstufe "Verbindung schließen" werden alle ein- und ausgehenden Netzwerkverbindungen blockiert. Dazu gehört auch der Zugriff auf Websites, E-Mails und Sicherheitsupdates. Diese Sicherheitsstufe hat die gleichen Auswirkungen wie das Trennen Ihrer Internetverbindung. Sie können diese Einstellung verwenden, um Ports zu blockieren, die im Bereich "Systemdienste" als geöffnet konfiguriert sind. Bei der Einstellung "Verbindung schließen" können weiterhin Warnungen angezeigt werden, in denen Sie aufgefordert werden, Programme zu sperren.

So setzen Sie die Firewall-Sicherheitsstufe auf "Verbindung schließen":

1. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" auf die Option **Erweitert**.
2. Stellen Sie den Schieberegler im Bereich "Sicherheitsstufe" so, dass **Verbindung schließen** als aktuelle Sicherheitsstufe angezeigt wird.
3. Klicken Sie auf **OK**.

Die Sicherheitsstufe "Stealth"

Bei der Firewall-Sicherheitsstufe "Stealth" werden alle eingehenden Netzwerkverbindungen mit Ausnahme der geöffneten Ports blockiert. Diese Einstellung verbirgt Ihren Computer vollständig gegenüber dem Internet. Bei der Firewall-Sicherheitsstufe "Stealth" werden Warnungen angezeigt, wenn neue Programme versuchen, auf das Internet zuzugreifen oder über eingehende Verbindungen Anfragen erhalten. Blockierte und hinzugefügte Anwendungen werden im Bereich "Programmberechtigungen" angezeigt.

So setzen Sie die Firewall-Sicherheitsstufe auf "Stealth":

1. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" auf die Option **Erweitert**.
2. Stellen Sie den Schieberegler im Bereich "Sicherheitsstufe" so, dass **Stealth** als aktuelle Sicherheitsstufe angezeigt wird.
3. Klicken Sie auf **OK**.

Die Sicherheitsstufe "Eingeschränkte Sicherheit"

Bei der Firewall-Sicherheitsstufe "Eingeschränkte Sicherheit" werden Sie informiert, wenn neue Programme versuchen, auf das Internet zuzugreifen oder über eingehende Verbindungen Anfragen erhalten. Blockierte und hinzugefügte Anwendungen werden im Bereich "Programmberechtigungen" angezeigt. Bei der Firewall-Sicherheitsstufe "Eingeschränkte Sicherheit" fordert ein Programm nur den Zugriffstyp an, den es zum aktuellen Zeitpunkt benötigt. So wird beispielsweise der Zugriff auf eine ausgehende Internetverbindung angefordert, den Sie entweder gewähren oder blockieren können. Benötigt das Programm zu einem späteren Zeitpunkt sowohl eine eingehende als auch eine ausgehende Verbindung, können Sie den uneingeschränkten Zugriff für das Programm im Bereich "Programmberechtigungen" gewähren.

So setzen Sie die Firewall-Sicherheitsstufe auf "Eingeschränkte Sicherheit":

1. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" auf die Option **Erweitert**.
2. Stellen Sie den Schieberegler im Bereich "Sicherheitsstufe" so, dass **Eingeschränkte Sicherheit** als aktuelle Sicherheitsstufe angezeigt wird.
3. Klicken Sie auf **OK**.

Die Sicherheitsstufe "Standardsicherheit"

Standardsicherheit ist die standardmäßige und empfohlene Sicherheitsstufe.

Bei der Firewall-Sicherheitsstufe "Standardsicherheit" überwacht Firewall eingehende und ausgehende Verbindungen und benachrichtigt Sie, wenn neue Programme versuchen, auf das Internet zuzugreifen. Blockierte und hinzugefügte Anwendungen werden im Bereich "Programmberechtigungen" angezeigt.

So setzen Sie die Firewall-Sicherheitsstufe auf "Standardsicherheit":

1. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" auf die Option **Erweitert**.
2. Stellen Sie den Schieberegler im Bereich "Sicherheitsstufe" so, dass **Standardsicherheit** als aktuelle Sicherheitsstufe angezeigt wird.
3. Klicken Sie auf **OK**.

Die Sicherheitsstufe "Vertrauenswürdige Sicherheit"

Bei der Firewall-Sicherheitsstufe "Vertrauenswürdige Sicherheit" werden alle eingehenden und ausgehenden Verbindungen gestattet. In dieser Einstellung gewährt Firewall automatisch allen Programmen Zugriff und fügt sie der Liste der zugelassenen Programme im Bereich "Programmberechtigungen" hinzu.

So setzen Sie die Firewall-Sicherheitsstufe auf "Vertrauenswürdige Sicherheit":

1. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" auf die Option **Erweitert**.
2. Stellen Sie den Schieberegler im Bereich "Sicherheitsstufe" so, dass **Vertrauenswürdige Sicherheit** als aktuelle Sicherheitsstufe angezeigt wird.
3. Klicken Sie auf **OK**.

Empfehlungen für Warnungen konfigurieren

Sie können Firewall so konfigurieren, dass Empfehlungen in die Warnungen zu Programmen, die auf das Internet zuzugreifen versuchen, aufgenommen, davon ausgeschlossen oder darin angezeigt werden.

Das Aktivieren der Option "Empfehlungen" unterstützt Sie bei der richtigen Vorgehensweise bei Warnungen. Wenn die Option "Empfehlungen" aktiviert ist (und die Sicherheitsstufe "Standardsicherheit" lautet), gewährt oder blockiert Firewall bekannte Programme automatisch. Darüber hinaus werden Sie beim Erkennen von unbekannten und potentiell schädlichen Programmen benachrichtigt und erhalten Vorschläge zu den erforderlichen Maßnahmen.

Ist die Option "Empfehlungen" hingegen deaktiviert, wird Firewall weder automatisch Internetzugriff gewähren oder blockieren noch erforderliche Maßnahmen empfehlen.

Wurde Firewall so konfiguriert, dass Empfehlungen nur angezeigt werden, fordert Sie die Warnung zum Gewähren oder Blockieren des Zugriffs auf, zeigt aber auch eine empfohlene Maßnahme an.

Empfehlungen aktivieren

Das Aktivieren der Option "Empfehlungen" unterstützt Sie bei der richtigen Vorgehensweise bei Warnungen. Wenn die Option "Empfehlungen" aktiviert ist, wird Firewall den Internetzugriff für Programme automatisch gewähren oder blockieren. Darüber hinaus werden Sie benachrichtigt, wenn unbekannte oder potentiell schädliche Programme erkannt werden.

So aktivieren Sie die Option "Empfehlungen":

1. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" auf die Option **Erweitert**.
2. Wählen Sie im Bereich "Sicherheitsstufe" unter **Empfehlungen** die Option **Aktivieren der Empfehlungen**.
3. Klicken Sie auf **OK**.

Empfehlungen deaktivieren

Wenn die Option "Empfehlungen" deaktiviert ist, enthalten die Warnungen keine Hinweise mehr zur Vorgehensweise bei Warnungen und zur Verwaltung des Zugriffs von Programmen. Ist die Option "Empfehlungen" deaktiviert, wird Firewall den Internetzugriff für Programme weiterhin gewähren oder blockieren. Darüber hinaus werden Warnungen angezeigt, wenn unbekannte oder potentiell schädliche Programme erkannt wurden. Erkennt Firewall dabei ein neues Programm, das verdächtig erscheint oder bei dem es sich um ein bekanntes schädliches Programm handelt, blockiert es automatisch den Zugriff dieses Programms auf das Internet.

So deaktivieren Sie die Option "Empfehlungen":

1. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" auf die Option **Erweitert**.
2. Wählen Sie im Bereich "Sicherheitsstufe" unter **Empfehlungen** die Option **Deaktivieren der Empfehlungen**.
3. Klicken Sie auf **OK**.

Nur Empfehlungen anzeigen

Das Anzeigen von Empfehlungen unterstützt Sie bei der richtigen Vorgehensweise bei Warnungen zu unbekannten und potentiell schädlichen Programmen. Ist die Option "Empfehlungen" auf **Nur Anzeige** gesetzt, werden zwar Informationen zur Vorgehensweise bei Warnungen angezeigt, aber im Gegensatz zur Option **Aktivieren der Empfehlungen** werden die angezeigten Empfehlungen nicht automatisch angewendet, und der Internetzugriff von Programmen wird nicht automatisch gestattet oder blockiert. Stattdessen unterstützen die Warnungen mit Empfehlungen Sie bei Ihrer Entscheidung, ob der Internetzugriff für bestimmte Programme gewährt oder blockiert werden soll.

So aktivieren Sie die Option "Nur Empfehlungen anzeigen":

1. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" auf die Option **Erweitert**.
2. Wählen Sie im Bereich "Sicherheitsstufe" unter **Empfehlungen** die Option **Nur Anzeige**.
3. Klicken Sie auf **OK**.

Firewall-Sicherheit optimieren

Es gibt viele Möglichkeiten, wie die Sicherheit Ihres Computers gefährdet werden könnte. Beispielsweise können einige Programme versuchen, eine Verbindung mit dem Internet herzustellen, bevor Windows(R) hochgefahren ist. Technisch versierte Anwender können ein ICMP-Echo-Request-Paket an Ihren Computer senden (pingen), um festzustellen, ob er an ein Netzwerk angeschlossen ist. Mit Firewall können Sie sich durch das Aktivieren eines Boot-Schutzes und das Blockieren von ICMP-Echo-Request-Anforderungen gegen beide Arten des Eindringens schützen. Der erste Schutzmechanismus blockiert den Zugriff von Programmen auf das Internet beim Hochfahren von Windows. Der zweite Mechanismus blockiert ICMP-Echo-Request-Anforderungen, mit denen ein anderer Benutzer feststellen kann, ob Ihr Computer mit dem Internet verbunden ist.

Zu den standardmäßigen Installationseinstellungen gehören das automatische Erkennen der am häufigsten auftretenden Einbruchsversuche, z. B. Denial-of-Service-Attacken oder Bedrohungen. Das Verwenden der standardmäßigen Installationseinstellungen gewährleistet, dass Sie vor diesen Angriffen und Prüfungen geschützt sind. Im Fenster zur Eindringungserkennung ("Intrusion Detection") haben Sie jedoch die Möglichkeit, das automatisch Erkennen von Angriffen oder Prüfungen zu deaktivieren.

Computer während des Hochfahrens schützen

Firewall kann Ihren Computer während des Hochfahrens von Windows schützen. Der Boot-Schutz blockiert alle neuen Programme, denen der Zugriff auf das Internet noch nicht gewährt wurde und die Zugriff auf das Internet anfordern. Nach dem Start von Firewall werden die entsprechenden Warnungen für die Programme angezeigt, die während des Hochfahrens einen Internetzugriff angefordert hatten. Jetzt können Sie diesen Zugriff entweder gewähren oder blockieren. Für diese Option darf Ihre Sicherheitsstufe jedoch nicht auf "Offen" oder "Verbindung schließen" eingestellt sein.

So schützen Sie Ihren Computer während des Hochfahrens:

1. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" auf die Option **Erweitert**.
2. Aktivieren Sie im Bereich "Sicherheitsstufe" unter "Sicherheitseinstellungen" die Option **Boot-Schutz aktivieren**.
3. Klicken Sie auf **OK**.

Hinweis: So lange der Boot-Schutz ausgeführt wird, werden keine blockierten Verbindungen und Intrusionsversuche protokolliert.

Einstellungen für ICMP-Echo-Request-Anforderungen konfigurieren

Technisch versierte Computerbenutzer können ein Ping-Tool verwenden, das ICMP-Echo-Request-Anforderungen sendet und empfängt, um festzustellen, ob ein bestimmter Computer mit dem Internet verbunden ist. Sie können Firewall so konfigurieren, dass Computerbenutzern das Anpingen Ihres Computers gestattet oder verweigert wird.

So konfigurieren Sie die ICMP-Echo-Request-Anforderungen:

1. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" auf die Option **Erweitert**.
2. Führen Sie im Bereich "Sicherheitsstufe" unter **Sicherheitseinstellungen** einen der folgenden Schritte aus:
   - Aktivieren Sie **ICMP-Pinganforderungen zulassen**, um die Erkennung Ihres Computers im Netzwerk durch das Senden von ICMP-Echo-Request-Anforderungen zu gestatten.

- Deaktivieren Sie **ICMP-Pinganforderungen zulassen**, um die Erkennung Ihres Computers im Netzwerk durch das Senden von ICMP-Echo-Request-Anforderungen zu verhindern.

3 Klicken Sie auf **OK**.

Erkennung von Intrusionsversuchen konfigurieren

Die Intrusionserkennung (IDS) prüft Datenpakete auf verdächtige Datenübertragungen oder Übertragungsmethoden. IDS analysiert den Datenverkehr und die Datenpakete auf bestimmte Datenverkehrsmuster, die von Angreifern verwendet werden. Wenn Firewall beispielsweise ICMP-Pakete erkennt, prüft es sie auf verdächtige Verkehrsmuster, indem es den ICMP-Datenverkehr mit den Mustern bekannter Angriffe vergleicht. Die Pakete werden mit einer Signaturdatenbank verglichen und automatisch verworfen, wenn sie von dem verdächtigen Computer stammen. Das Ereignis kann optional protokolliert werden.

Zu den standardmäßigen Installationseinstellungen gehören das automatische Erkennen der am häufigsten auftretenden Einbruchsversuche, z. B. Denial-of-Service-Attacken oder Bedrohungen. Das Verwenden der standardmäßigen Installationseinstellungen gewährleistet, dass Sie vor diesen Angriffen und Prüfungen geschützt sind. Im Fenster zur Eindringungserkennung ("Intrusion Detection") haben Sie jedoch die Möglichkeit, das automatisch Erkennen von Angriffen oder Prüfungen zu deaktivieren.

So konfigurieren Sie die Erkennung von Intrusionsversuchen:

1 Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" auf die Option **Erweitert**.

2 Klicken Sie im Bereich "Firewall" auf **Intrusionserkennung**.

3 Führen Sie unter **Intrusionsversuche erkennen** einen der folgenden Schritte aus:

- Wählen Sie einen Namen, um einen Angriff oder Scan-Versuch automatisch zu erkennen.
- Entfernen Sie einen Namen, um die automatische Erkennung eines Angriffs oder Scan-Versuchs zu deaktivieren.

4 Klicken Sie auf **OK**.

Statuseinstellungen für den Firewall-Schutz konfigurieren

SecurityCenter verfolgt Probleme, die ein Teil Ihres allgemeinen Computer-Schutzstatus darstellen. Sie können Firewall jedoch so konfigurieren, dass bestimmte Probleme auf Ihrem Computer, die den Schutzstatus beeinflussen könnten, ignoriert werden. Sie können SecurityCenter so konfigurieren, dass es eine Einstellung der Sicherheitsstufe von "Offen" ignoriert, wenn der Firewall-Dienst nicht ausgeführt wird und keine Firewall für ausgehenden Datenverkehr auf Ihrem Computer installiert ist.

So konfigurieren Sie die Statuseinstellungen für den Firewall-Schutz:

1. Klicken Sie im Fenster "Häufige Tasks" auf das Menü **Erweitert**.
2. Klicken Sie auf **Konfigurieren**.
3. Klicken Sie im Fenster zur SecurityCenter-Konfiguration auf **Warnungen**.
4. Klicken Sie auf **Erweitert**.
5. Klicken Sie im Bereich "Häufige Tasks" auf das Menü **Erweitert**.
6. Klicken Sie auf **Konfigurieren**.
7. Klicken Sie im Bereich "SecurityCenter-Konfiguration" auf die Option **Schutzstatus**.
8. Klicken Sie auf "Erweitert".
9. Wählen Sie im Bereich "Ignorierte Probleme" eine oder mehrere der folgenden Optionen:
   - **Die Firewall ist auf die Sicherheitsstufe "Offen" eingestellt.**
   - **Der Firewall-Dienst wird nicht ausgeführt.**
   - **Auf Ihrem Computer ist keine Firewall für ausgehenden Datenverkehr vorhanden.**
10. Klicken Sie auf **OK**.

Firewall sperren und wiederherstellen

Das Sperren der Firewall ist bei folgenden Situationen hilfreich: bei der Bearbeitung von computerbezogenen Notfällen; für Benutzer, die den gesamten Verkehr sperren müssen, um ein Problem auf ihrem Computer zu isolieren und zu beheben; oder für Benutzer, die unsicher sind und entscheiden müssen, wie der Zugriff eines Programms auf das Internet gehandhabt werden soll.

Firewall sofort sperren

Durch das Sperren der Firewall wird der gesamte eingehende und ausgehende Datenverkehr zwischen Ihrem Computer und dem Internet sofort blockiert. Allen Remote-Verbindungen wird der Zugriff auf Ihren Computer verweigert, und alle Programme auf Ihrem Computer können nicht mehr auf das Internet zugreifen.

So sperren Sie die Firewall sofort und blockieren den gesamten Internetdatenverkehr:

1. Aktivieren Sie im Bereich "Startseite" oder "Häufige Tasks" bei aktiviertem Menü **Grundlagen** oder **Erweitert** die Option **Firewall sperren**.
2. Klicken Sie im Bereich "Firewall sperren" auf **Schließen**.
3. Klicken Sie im Dialogfeld auf **Ja**, um das sofortige Sperren des gesamten eingehenden und ausgehenden Datenverkehrs zu bestätigen.

Firewall-Sperre sofort aufheben

Durch das Sperren der Firewall wird der gesamte eingehende und ausgehende Datenverkehr zwischen Ihrem Computer und dem Internet sofort blockiert. Allen Remote-Verbindungen wird der Zugriff auf Ihren Computer verweigert, und alle Programme auf Ihrem Computer können nicht mehr auf das Internet zugreifen. Nachdem Sie den Befehl "Firewall sperren" gewählt haben, können Sie die Sperre wieder aufheben, um den Internetdatenverkehr wieder zuzulassen.

So heben Sie die Firewall-Sperre sofort auf und gestatten den gesamten Internetdatenverkehr:

1. Aktivieren Sie im Bereich "Startseite" oder "Häufige Tasks" bei aktiviertem Menü **Grundlagen** oder **Erweitert** die Option **Firewall sperren**.
2. Klicken Sie im Bereich "Sperrung aktiviert" auf **Sperre aufheben**.
3. Klicken Sie im Dialogfeld auf **Ja**, um das sofortige Aufheben der Sperre des gesamten eingehenden und ausgehenden Datenverkehrs zu bestätigen.

Firewall-Standardeinstellungen wiederherstellen

Sie können die Standard-Sicherheitseinstellungen der Firewall schnell und einfach wiederherstellen. Dabei wird Ihre Sicherheitsstufe auf "Standardsicherheit" gesetzt, die Option "Empfehlungen" wird aktiviert, vertrauenswürdige und gesperrte IP-Adressen werden zurückgesetzt, und es werden alle Programme aus dem Fensterbereich "Programmberechtigungen" entfernt.

So stellen Sie die Standardeinstellungen der Firewall wieder her:

1. Aktivieren Sie im Bereich "Startseite" oder "Häufige Tasks" bei aktiviertem Menü **Grundlagen** oder **Erweitert** die Option **Standardwerte für Firewall wiederherstellen**.
2. Klicken Sie im Bereich "Standardwerte für Firewall-Schutz wiederherstellen" auf **Standardeinstellungen wiederherstellen**.
3. Klicken Sie im Dialogfeld "Standardwerte für Firewall-Schutz wiederherstellen" auf **Ja**, um das Wiederherstellen der Firewall-Standardeinstellungen zu bestätigen.

Die Sicherheitsstufe "Offen"

Bei der Sicherheitsstufe "Offen" gestattet die Firewall den Zugriff auf alle eingehenden und ausgehenden Verbindungen. In dem Bereich "Programmberechtigungen" können Sie den Zugriff auch für zuvor blockierte Programme gewähren.

So setzen Sie die Firewall-Sicherheitsstufe auf "Offen":

1. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" auf die Option **Erweitert**.
2. Stellen Sie den Schieberegler im Bereich "Sicherheitsstufe" so, dass **Offen** als aktuelle Sicherheitsstufe angezeigt wird.
3. Klicken Sie auf **OK**.

Hinweis: Wenn die Firewall-Sicherheitsstufe auf **Offen** eingestellt ist, werden zuvor blockierte Programme auch weiterhin blockiert. Sie können dies durch Ändern der Programmregel auf **Vollzugriff** verhindern.

KAPITEL 20

Programme und Berechtigungen verwalten

Mit Firewall können Sie Zugriffsberechtigungen für bereits vorhandene und neue Programme, die Zugriff auf eingehende und ausgehende Internetverbindungen benötigen, verwalten und erstellen. Sie können Programmen den vollständigen Zugriff oder nur den Zugriff auf ausgehende Verbindungen gewähren. Alternativ können Sie Programmen den Zugriff auf Internetverbindungen dauerhaft blockieren.

In diesem Kapitel

Internetzugriff für Programme gewähren 148
Programmen nur den Zugriff auf ausgehende Verbindungen gewähren 152
Internetzugriff für Programme blockieren 155
Zugriffsberechtigungen für Programme entfernen .. 158
Weitere Informationen zu Programmen abrufen 159

Internetzugriff für Programme gewähren

Einige Programme, wie z. B. Internetbrowser, müssen auf das Internet zugreifen können, um ihre eigentliche Funktion ausführen zu können.

Dazu können Sie im Bereich "Programmberechtigungen" von Firewall die folgenden Einstellungen vornehmen:

- Programmen den Zugriff auf Internetverbindungen gewähren
- Programmen den Zugriff nur auf ausgehende Verbindungen gewähren
- Programmen den Zugriff auf Internetverbindungen sperren

Die Zugriffsarten "Vollständig" und "Nur ausgehender Zugriff" können Sie auch aus den Protokollen "Ausgehende Ereignisse" und "Zuletzt aufgetretene Ereignisse" gewähren.

Uneingeschränkten Zugriff für ein Programm gewähren

Viele Programme auf Ihrem Computer benötigen Zugriff auf eingehende und ausgehende Internetverbindungen. Personal Firewall enthält eine Liste mit Programmen, denen der vollständige Zugriff automatisch gewährt wird. Diese Berechtigungen können Sie bei Bedarf auch bearbeiten.

So gewähren Sie einem Programm den uneingeschränkten Internetzugriff:

1. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" auf die Option **Erweitert**.
2. Klicken Sie im Bereich "Firewall" auf **Programmberechtigungen**.
3. Wählen Sie unter **Programmberechtigungen** ein Programm mit dem Status **Blockiert** oder **Nur ausgehender Zugriff** aus.
4. Klicken Sie unter **Aktion** auf **Vollständigen Zugriff gewähren**.
5. Klicken Sie auf **OK**.

Vollständigen Zugriff für ein neues Programm gewähren

Viele Programme auf Ihrem Computer benötigen Zugriff auf eingehende und ausgehende Internetverbindungen. Personal Firewall enthält eine Liste mit Programmen, denen der vollständige Zugriff automatisch gewährt wird. Dieser Liste können Sie ein neues Programm hinzufügen und die Berechtigungen konfigurieren.

So gewähren Sie einem neuen Programm den uneingeschränkten Internetzugriff:

1. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" auf die Option **Erweitert**.
2. Klicken Sie im Bereich "**Firewall** " auf **Programmberechtigungen**.
3. Klicken Sie unter **Programmberechtigungen** auf **Erlaubtes Programm hinzufügen**.
4. Wählen Sie im Dialogfeld **Programm hinzufügen** das Programm aus, das Sie hinzufügen möchten.
5. Klicken Sie auf **Öffnen**.
6. Klicken Sie auf **OK**.

   Das neu hinzugefügte Programm wird jetzt im Bereich **Programmberechtigungen** angezeigt.

Hinweis: Sie können die Berechtigungen eines neu hinzugefügten Programms auf die gleiche Weise wie die eines bereits vorhandenen Programms ändern. Dazu wählen Sie das Programm aus und klicken dann unter **Aktion** auf **Nur ausgehenden Zugriff gewähren** oder **Zugriff blockieren**.

Uneingeschränkten Zugriff aus dem Protokoll "Zuletzt aufgetretene Ereignisse" gewähren

Viele Programme auf Ihrem Computer benötigen Zugriff auf eingehende und ausgehende Internetverbindungen. Diese Art des Zugriffs können Sie auch zuweisen, indem Sie ein Programm im Protokoll "Zuletzt aufgetretene Ereignisse" auswählen und den Status "Vollständig" zuweisen.

So gewähren Sie einem Programm uneingeschränkten Zugriff über das Protokoll "Zuletzt aufgetretene Ereignisse":

1. Klicken Sie im Fenster "Häufige Tasks" auf **Berichte & Protokolle**.
2. Wählen Sie unter "Zuletzt aufgetretene Ereignisse" eine Ereignisbeschreibung aus, und klicken Sie dann auf **Uneingeschränkten Zugriff gewähren**.
3. Klicken Sie im Dialogfeld "Programmberechtigungen" auf **Ja**, um den vollständigen Internetzugriff des Programms zu bestätigen.

Verwandte Themen

- Ausgehende Ereignisse anzeigen (Seite 183)

Uneingeschränkten Zugriff aus dem Protokoll "Ausgehende Ereignisse" gewähren

Viele Programme auf Ihrem Computer benötigen Zugriff auf eingehende und ausgehende Internetverbindungen. Diese Art des Zugriffs können Sie auch zuweisen, indem Sie ein Programm im Protokoll "Ausgehende Ereignisse" auswählen und ihm den Status "Vollständig" zuweisen.

So gewähren Sie einem Programm uneingeschränkten Zugriff über das Protokoll "Ausgehende Ereignisse":

1. Klicken Sie im Fenster "Häufige Tasks" auf **Berichte & Protokolle**.
2. Klicken Sie unter **Zuletzt aufgetretene Ereignisse** auf **Protokoll anzeigen**.
3. Wählen Sie **Internet & Netzwerk** und anschließend **Ausgehende Ereignisse**.
4. Wählen Sie im Bereich "Ausgehende Ereignisse" eine Quell-IP-Adresse aus, und klicken Sie dann auf **Zugriff gewähren**.
5. Klicken Sie im Dialogfeld "Programmberechtigungen" auf **Ja**, um den vollständigen Internetzugriff des Programms zu bestätigen.

Verwandte Themen

- Ausgehende Ereignisse anzeigen (Seite 183)

Programmen nur den Zugriff auf ausgehende Verbindungen gewähren

Viele Programme auf Ihrem Computer benötigen nur Zugriff auf ausgehende Internetverbindungen. Sie können diesen Programmen nur den Zugriff auf ausgehende Verbindungen gewähren.

Zugriff auf ausgehende Verbindungen für ein Programm gewähren

Viele Programme auf Ihrem Computer benötigen Zugriff auf eingehende und ausgehende Internetverbindungen. Personal Firewall enthält eine Liste mit Programmen, denen der vollständige Zugriff automatisch gewährt wird. Diese Berechtigungen können Sie bei Bedarf auch bearbeiten.

So gewähren Sie einem Programm nur Zugriff auf ausgehenden Verkehr:

1. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" auf die Option **Erweitert**.
2. Klicken Sie im Bereich "Firewall" auf **Programmberechtigungen**.
3. Wählen Sie unter **Programmberechtigungen** ein Programm mit dem Status **Blockiert** oder **Vollständig** aus.
4. Klicken Sie unter **Aktion** auf **Nur ausgehenden Zugriff gewähren**.
5. Klicken Sie auf **OK**.

Nur ausgehenden Zugriff aus dem Protokoll "Zuletzt aufgetretene Ereignisse" gewähren

Viele Programme auf Ihrem Computer benötigen Zugriff auf eingehende und ausgehende Internetverbindungen. Diese Art des Zugriffs können Sie auch zuweisen, indem Sie ein Programm im Protokoll "Zuletzt aufgetretene Ereignisse" auswählen und den Status "Nur ausgehenden Zugriff" zuweisen.

So gewähren Sie einem Programm nur ausgehenden Zugriff über das Protokoll "Zuletzt aufgetretene Ereignisse":

1. Klicken Sie im Fenster "Häufige Tasks" auf **Berichte & Protokolle**.
2. Wählen Sie unter "Zuletzt aufgetretene Ereignisse" eine Ereignisbeschreibung aus, und klicken Sie dann auf **Nur ausgehenden Zugriff gewähren**.
3. Klicken Sie im Dialogfeld "Programmberechtigungen" auf **Ja**, um den Zugriff nur auf ausgehende Internetverbindungen des Programms zu bestätigen.

Verwandte Themen

- Ausgehende Ereignisse anzeigen (Seite 183)

Nur ausgehenden Zugriff aus dem Protokoll "Ausgehende Ereignisse" gewähren

Viele Programme auf Ihrem Computer benötigen Zugriff auf eingehende und ausgehende Internetverbindungen. Diese Art des Zugriffs können Sie auch zuweisen, indem Sie ein Programm im Protokoll "Ausgehende Ereignisse" auswählen und ihm den Status "Nur ausgehenden Zugriff" zuweisen.

So gewähren Sie einem Programm nur ausgehenden Zugriff über das Protokoll "Ausgehende Ereignisse":

1. Klicken Sie im Fenster "Häufige Tasks" auf **Berichte & Protokolle**.
2. Klicken Sie unter **Zuletzt aufgetretene Ereignisse** auf **Protokoll anzeigen**.
3. Wählen Sie **Internet & Netzwerk** und anschließend **Ausgehende Ereignisse**.
4. Wählen Sie im Bereich "Ausgehende Ereignisse" eine Quell-IP-Adresse und klicken Sie dann auf **Nur ausgehenden Zugriff gewähren**.
5. Klicken Sie im Dialogfeld "Programmberechtigungen" auf **Ja**, um den Zugriff nur auf ausgehende Internetverbindungen des Programms zu bestätigen.

Verwandte Themen

- Ausgehende Ereignisse anzeigen (Seite 183)

Internetzugriff für Programme blockieren

Sie können bestimmten Programmen den Zugriff auf das Internet sperren. Durch das Blockieren des Internetzugriffs für ein Programm stellen Sie sicher, dass Ihre Netzwerkverbindung oder ein anderes Programm, das eine Internetverbindung für die ordnungsgemäße Funktion benötigt, nicht unterbrochen wird.

Zugriff für ein Programm sperren

Viele Programme auf Ihrem Computer benötigen Zugriff auf eingehende und ausgehende Internetverbindungen. Personal Firewall enthält eine Liste mit Programmen, denen der vollständige Zugriff automatisch gewährt wird. Diese Berechtigungen können von Ihnen gesperrt werden.

So sperren Sie den Internetzugriff für ein Programm:

1. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" auf die Option **Erweitert**.
2. Klicken Sie im Bereich "Firewall" auf **Programmberechtigungen**.
3. Wählen Sie unter **Programmberechtigungen** ein Programm mit dem Status **Vollzugriff** oder **Nur ausgehender Zugriff** aus.
4. Klicken Sie unter **Aktion** auf **Zugriff blockieren**.
5. Klicken Sie auf **OK**.

Zugriff für ein neues Programm sperren

Viele Programme auf Ihrem Computer benötigen Zugriff auf eingehende und ausgehende Internetverbindungen. Personal Firewall enthält eine Liste mit Programmen, denen der Zugriff automatisch gesperrt wird. Dieser Liste können Sie ein neues Programm hinzufügen und den Zugriff auf das Internet sperren.

So sperren Sie den Internetzugriff für ein neues Programm:

1. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" auf die Option **Erweitert**.
2. Klicken Sie im Bereich "Firewall" auf **Programmberechtigungen**.
3. Klicken Sie unter **Programmberechtigungen** auf **Blockiertes Programm hinzufügen**.
4. Wählen Sie im Dialogfeld **Programm hinzufügen** das Programm aus, das Sie hinzufügen möchten.
5. Klicken Sie auf **Öffnen**.
6. Klicken Sie auf **OK**.

   Das neu hinzugefügte Programm wird jetzt im Bereich **Programmberechtigungen** angezeigt.

Hinweis: Sie können die Berechtigungen eines neu hinzugefügten Programms auf die gleiche Weise wie die eines bereits vorhandenen Programms ändern. Dazu wählen Sie das Programm aus und klicken dann unter **Aktion** auf **Nur ausgehenden Zugriff gewähren** oder **Vollständigen Zugriff gewähren**.

Zugriff aus dem Protokoll "Zuletzt aufgetretene Ereignisse" blockieren

Viele Programme auf Ihrem Computer benötigen Zugriff auf eingehende und ausgehende Internetverbindungen. Jedoch können Sie Programmen den Zugriff auf das Internet aus dem Protokoll "Zuletzt aufgetretene Ereignisse" sperren.

So sperren Sie den Internetzugriff eines Programms aus dem Protokoll "Zuletzt aufgetretene Ereignisse":

1. Klicken Sie im Fenster "Häufige Tasks" auf **Berichte & Protokolle**.
2. Wählen Sie unter "Zuletzt aufgetretene Ereignisse" eine Ereignisbeschreibung aus und klicken Sie dann auf **Zugriff blockieren**.
3. Klicken Sie im Dialogfeld "Programmberechtigungen" auf **Ja**, um das Sperren des Internetzugriffs für ein Programm zu bestätigen.

Verwandte Themen

- Ausgehende Ereignisse anzeigen (Seite 183)

Zugriffsberechtigungen für Programme entfernen

Bevor Sie eine Programmberechtigung eines Programms entfernen, müssen Sie überprüfen, ob das Sperren des Internetzugriffs für dieses Programm negative Auswirkungen auf die Funktionen des Computers oder des Netzwerks hat.

Programmberechtigung entfernen

Viele Programme auf Ihrem Computer benötigen Zugriff auf eingehende und ausgehende Internetverbindungen. Personal Firewall enthält eine Liste mit Programmen, denen der vollständige Zugriff automatisch gewährt wird. Sie können automatisch oder manuell hinzugefügte Programme jedoch auch wieder aus dieser Liste entfernen.

So entfernen Sie die Programmberechtigung für ein neues Programm:

1. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" auf die Option **Erweitert**.
2. Klicken Sie im Bereich "Firewall" auf **Programmberechtigungen**.
3. Wählen Sie unter **Programmberechtigungen** ein Programm aus.
4. Klicken Sie unter **Aktion** auf **Programmberechtigung löschen**.
5. Klicken Sie auf **OK**.

   Das Programm wird aus dem Bereich "Programmberechtigungen" Liste entfernt.

Hinweis: Durch Abblenden und Deaktivieren von Aktionen verhindert Firewall, dass Sie die Berechtigung von bestimmten Programmen ändern.

Weitere Informationen zu Programmen abrufen

Wenn Sie nicht sicher sind, welche Programmberechtigung für ein bestimmtes Programm gelten soll, können Sie entsprechende Informationen zu diesem Programm auf McAfees Hackerwatch-Website nachlesen.

Programminformationen erhalten

Viele Programme auf Ihrem Computer benötigen Zugriff auf eingehende und ausgehende Internetverbindungen. Personal Firewall enthält eine Liste mit Programmen, denen der vollständige Zugriff automatisch gewährt wird. Diese Berechtigungen können Sie bei Bedarf auch bearbeiten.

Firewall kann Ihnen bei Ihrer Entscheidung helfen, ob Sie einem Programm den Internetzugriff gewähren oder sperren sollen. Stellen Sie sicher, dass Sie eine Verbindung mit dem Internet hergestellt haben, so dass Ihr Browser die Hackerwatch-Website von McAfee aufrufen kann. Auf dieser Website finden Sie aktuelle Informationen zu Programmen, den Anforderungen an den Internetzugriff sowie bekannte Sicherheitsrisiken.

So erhalten Sie Programminformationen:

1. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" auf die Option **Erweitert**.
2. Klicken Sie im Bereich "Firewall" auf **Programmberechtigungen**.
3. Wählen Sie unter **Programmberechtigungen** ein Programm aus.
4. Klicken Sie unter **Aktion** auf **Weitere Informationen**.

Weitere Programminformationen aus dem Protokoll "Ausgehende Ereignisse" abrufen

Mit Personal Firewall können Sie weitere Informationen zu Programmen abrufen, die in dem Protokoll "Ausgehende Ereignisse" aufgeführt sind.

Bevor Sie Informationen zu einem Programm abrufen, stellen Sie sicher, dass eine Internetverbindung besteht und Sie über einen Internetbrowser verfügen.

So rufen Sie weitere Programminformationen aus dem Protokoll "Ausgehende Ereignisse" ab:

1. Klicken Sie im Fenster "Häufige Tasks" auf **Berichte & Protokolle**.
2. Klicken Sie unter **Zuletzt aufgetretene Ereignisse** auf **Protokoll anzeigen**.
3. Wählen Sie **Internet & Netzwerk** und anschließend **Ausgehende Ereignisse**.
4. Wählen Sie im Bereich "Ausgehende Ereignisse" eine Quell-IP-Adresse aus und klicken Sie dann auf **Weitere Informationen**.

   Sie können weitere Informationen zu einem gewünschten Programm auf der Hackerwatch-Website anzeigen. Hackerwatch bietet Ihnen aktuelle Informationen zu Programmen, deren Anforderungen an den Internetzugriff sowie bekannte Sicherheitsrisiken.

Verwandte Themen

- Ausgehende Ereignisse anzeigen (Seite 183)

KAPITEL 21

Systemdienste verwalten

Einige Programme, beispielsweise Webserver oder Serverprogrammen für die Dateifreigabe, müssen für eine ordnungsgemäße Funktion nicht angeforderte Verbindungen von anderen Computern akzeptieren, die über bestimmte Systemdienstports eingehen. In der Regel schließt Firewall diese Systemdienstports, da sie eine mögliche Quelle für Sicherheitsrisiken in Ihrem System darstellen. Diese Systemdienstports müssen jedoch offen sein, damit Verbindungen von Remote-Computern akzeptiert werden können.

Die folgende Liste enthält die Standardports für allgemeine Dienste.

- File Transfer Protocol (FTP) Ports 20-21
- Mail Server (IMAP) Port 143
- Mail Server (POP3) Port 110
- Mail Server (SMTP) Port 25
- Microsoft Directory Server (MSFT DS) Port 445
- Microsoft SQL Server (MSFT SQL) Port 1433
- Remoteunterstützung / Terminalserver (RDP) Port 3389
- Remoteprozeduraufrufe (RPC) Port 135
- Secure Web Server (HTTPS) Port 443
- Universal Plug and Play (UPNP) Port 5000
- Web Server (HTTP) Port 80
- Windows-Dateifreigabe (NETBIOS) Ports 137-139

In diesem Kapitel

Systemdienstports konfigurieren.....162

Systemdienstports konfigurieren

Damit ein Remotezugriff auf einen Dienst auf Ihrem Computer zustande kommen kann, müssen Sie den Dienst angeben und den zugehörigen Port als offen deklarieren. Wählen Sie einen Dienst und einen Port nur dann aus, wenn Sie sich sicher sind, dass der Port offen sein muss. Es ist nur selten notwenig, dass Sie einen Port öffnen.

Zugriff auf einen vorhandenen Systemdienstport gewähren

Im Fenster "Systemdienste" können Sie einen Anschluss öffnen oder schließen, um den Remote-Zugriff auf einen Netzwerkdienst auf Ihrem Computer zuzulassen oder abzulehnen. Ein offener Systemdienstanschluss kann für Ihren Computer ein Sicherheitsrisiko gegen Bedrohungen aus dem Internet darstellen. Öffnen Sie einen Anschluss daher nur, wenn dies erforderlich ist.

So gewähren Sie den Zugriff auf einen vorhandenen Systemdienstport:

1. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" auf die Option **Erweitert**.
2. Klicken Sie im Bereich "Firewall" auf **Systemdienste**.
3. Wählen Sie unter **Offener Systemdienstport** einen Systemdienst aus, um einen zugehörigen Port zu öffnen.
4. Klicken Sie auf **OK**.

Zugriff auf einen vorhandenen Systemdienstport sperren

Im Fenster "Systemdienste" können Sie einen Anschluss öffnen oder schließen, um den Remote-Zugriff auf einen Netzwerkdienst auf Ihrem Computer zuzulassen oder abzulehnen. Ein offener Systemdienstanschluss kann für Ihren Computer ein Sicherheitsrisiko gegen Bedrohungen aus dem Internet darstellen. Öffnen Sie einen Anschluss daher nur, wenn dies erforderlich ist.

So sperren Sie den Zugriff auf einen vorhandenen Systemdienstport:

1. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" auf die Option **Erweitert**.
2. Klicken Sie im Bereich "Firewall" auf **Systemdienste**.
3. Wählen Sie unter **Offener Systemdienstport** einen Systemdienst aus, um einen zugehörigen Port zu schließen.
4. Klicken Sie auf **OK**.

Neuen Systemdienstport konfigurieren

Im Bereich "Systemdienste" können Sie einen neuen Systemdienstport hinzufügen, den Sie dann öffnen oder schließen können, um den Remotezugriff auf einen Netzwerkdienst auf Ihrem Computer zu gestatten oder zu verweigern. Offene Systemdienstports stellen ein Sicherheitsrisiko für Ihren Computer gegenüber Bedrohungen aus dem Internet dar, daher sollten Sie einen Port nur dann öffnen, wenn es unbedingt notwendig ist.

So erstellen und konfigurieren Sie einen neuen Systemdienstport:

1. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" auf die Option **Erweitert**.
2. Klicken Sie im Bereich "Firewall" auf **Systemdienste**.
3. Klicken Sie auf **Hinzufügen**.
4. Geben Sie unter **Portkonfiguration hinzufügen** Folgendes an:
   - Programmname
   - Eingehende TCP/IP-Ports
   - Ausgehende TCP/IP-Ports
   - Eingehende UDP-Ports
   - Ausgehende UDP-Ports
5. Geben Sie optional eine Beschreibung für die neue Konfiguration ein.
6. Klicken Sie auf **OK**.

   Der neu konfigurierte Systemdienstport wird unter **Offener Systemdienstport** angezeigt.

Systemdienstport bearbeiten

Ein offener bzw. geschlossener Port gestattet bzw. verweigert den Zugriff auf einen Netzwerkdienst auf Ihrem Computer. Im Bereich "Systemdienste" können Sie die Informationen für eingehende und ausgehende Verbindungen eines vorhandenen Portes bearbeiten. Wenn die Portinformationen falsch eingegeben werden, kann der Systemdienst nicht ordnungsgemäß arbeiten.

So bearbeiten Sie einen Systemdienstport:

1. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" auf die Option **Erweitert**.
2. Klicken Sie im Bereich "Firewall" auf **Systemdienste**.
3. Wählen Sie einen Systemdienst aus und klicken Sie dann auf **Bearbeiten**.
4. Geben Sie unter **Portkonfiguration hinzufügen** Folgendes an:
   - Programmname
   - Eingehende TCP/IP-Ports
   - Ausgehende TCP/IP-Ports
   - Eingehende UDP-Ports
   - Ausgehende UDP-Ports
5. Geben Sie optional eine Beschreibung für die geänderte Konfiguration ein.
6. Klicken Sie auf **OK**.

   Der geänderte Systemdienstport wird unter **Offener Systemdienstport** angezeigt.

Systemdienstport entfernen

Ein offener bzw. geschlossener Port gestattet oder verweigert den Zugriff auf einen Netzwerkdienst auf Ihrem Computer. Im Bereich "Systemdienste" können Sie einen vorhandenen Port und den dazugehörigen Systemdienst entfernen. Wenn ein Port und der dazugehörigen Systemdienst aus dem Bereich "Systemdienste" entfernt wurden, können Remote-Computer nicht mehr auf einen Netzwerkdienst auf Ihrem Computer zugreifen.

So entfernen Sie einen Systemdienstport:

1. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" auf die Option **Erweitert**.
2. Klicken Sie im Bereich "Firewall" auf **Systemdienste**.
3. Wählen Sie einen Systemdienst aus und klicken Sie dann auf **Entfernen**.
4. Klicken Sie im Dialogfeld **Programmberechtigungen** auf**Ja**, um das Löschen des Systemdienstes zu bestätigen.

   Der Systemdienstport wird nicht mehr im Bereich "Systemdienste" angezeigt.

KAPITEL 22

Computerverbindungen verwalten

Sie können Firewall so konfigurieren, dass bestimmte Remote-Verbindungen mit Ihrem Computer über Richtlinien verwaltet werden, die auf den IP-Adressen basieren, die diesen Remote-Computern zugeordnet sind. Computer, denen vertrauenswürdige IP-Adressen zugeordnet sind, dürfen eine Verbindung mit Ihrem Computer herstellen. Computer, deren IP-Adressen unbekannt, verdächtig oder nicht vertrauenswürdig sind, kann das Herstellen einer Verbindung mit Ihrem Computer verweigert werden.

Wenn Sie eine Verbindung zulassen, stellen Sie sicher, dass der Computer, den Sie als vertrauenswürdig einstufen, sicher ist. Wenn ein Computer, den Sie als vertrauenswürdig einstufen, durch einen Wurm oder auf andere Weise infiziert wird, besteht für Ihren Computer möglicherweise ebenfalls ein Risiko. McAfee empfiehlt zudem, dass der bzw. die Computer, die Sie als vertrauenswürdig einstufen, durch eine Firewall und ein aktuelles Antivirusprogramm zu schützen. Für alle IP-Adressen, die in der Liste der vertrauenswürdigen IP-Adressen enthalten sind, protokolliert Firewall weder den Datenverkehr noch generiert es Ereigniswarnungen.

Sie können sicherstellen, dass Computer, die mit unbekannten, verdächtigen oder nicht vertrauenswürdigen IP-Adressen in Verbindung gebracht werden, keine Verbindung zu Ihrem Computer herstellen können.

Da Firewall jeglichen unerwünschten Verkehr blockiert, ist es in der Regel nicht erforderlich, eine IP-Adresse zu sperren. Sie sollten eine IP-Adresse nur dann sperren, wenn Sie sicher sind, dass eine Internetverbindung eine spezifische Bedrohung darstellt. Stellen Sie sicher, dass Sie keine wichtigen IP-Adressen sperren, wie z. B. DNS- bzw. DHCP-Server oder andere Server Ihres ISP. Je nach Ihren Sicherheitseinstellungen kann Firewall Sie benachrichtigen, wenn es ein von einem gesperrten Computer stammendes Ereignis erkennt.

In diesem Kapitel

Vertrauenswürdige Computerverbindungen.....168
Sperren von Computerverbindungen 173

Vertrauenswürdige Computerverbindungen

Sie können vertrauenswürdige IP-Adressen im Bereich "Vertrauenswürdige und gesperrte IPs" unter **Vertrauenswürdige IP-Adressen** hinzufügen, bearbeiten und entfernen.

In der Liste **Vertrauenswürdige IP-Adressen** im Fenster "Vertrauenswürdige und gesperrte IP-Adressen". Für IP-Adressen, die in der Liste **Vertrauenswürdige IP-Adressen** angezeigt werden, protokolliert Firewall weder Verkehr noch generiert es Ereigniswarnungen.

Firewall vertraut allen geprüften IP-Adressen in der Liste und gewährt den Datenverkehr, der von diesen IP-Adressen stammt, über jeden Port. Firewall protokolliert keine Ereignisse von vertrauenswürdigen IP-Adressen. Aktivitäten zwischen Computern, denen eine vertrauenswürdige IP Adresse zugeordnet ist und Ihrem Computer werden von Firewall weder gefiltert noch analysiert.

Wenn Sie eine Verbindung zulassen, stellen Sie sicher, dass der Computer, den Sie als vertrauenswürdig einstufen, sicher ist. Wenn ein Computer, den Sie als vertrauenswürdig einstufen, durch einen Wurm oder auf andere Weise infiziert wird, besteht für Ihren Computer möglicherweise ebenfalls ein Risiko. McAfee empfiehlt zudem, dass der bzw. die Computer, die Sie als vertrauenswürdig einstufen, durch eine Firewall und ein aktuelles Antivirusprogramm zu schützen.

Vertrauenswürdige Computerverbindung hinzufügen

Sie können eine vertrauenswürdige Computerverbindung und die dazugehörige IP-Adresse hinzufügen.

In der Liste **Vertrauenswürdige IP-Adressen** im Fenster "Vertrauenswürdige und gesperrte IP-Adressen". Für IP-Adressen, die in der Liste **Vertrauenswürdige IP-Adressen** angezeigt werden, protokolliert Firewall weder Verkehr noch generiert es Ereigniswarnungen.

Computer mit vertrauenswürdigen IP-Adressen können jederzeit eine Verbindung mit Ihrem Computer herstellen. Bevor Sie eine vertrauenswürdige IP-Adresse hinzufügen, bearbeiten oder entfernen, stellen Sie sicher, dass es sich um eine IP-Adresse handelt, über die eine sichere Kommunikation gewährleistet ist bzw. die sicher entfernt werden kann.

So fügen Sie eine vertrauenswürdige Computerverbindung hinzu:

1. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" auf die Option **Erweitert**.
2. Klicken Sie im Bereich "Firewall" auf **Vertrauenswürdige und gesperrte IPs**.
3. Wählen Sie im Bereich "Vertrauenswürdige und gesperrte IPs" die Option **Vertrauenswürdige IP-Adressen**.
4. Klicken Sie auf **Hinzufügen**.
5. Führen Sie unter **Regel für vertrauenswürdige IP-Adresse** einen der folgenden Schritte aus:
   - Wählen Sie eine **Einzelne IP-Adresse** aus und geben Sie dann die IP-Adresse ein.
   - Wählen Sie einen **IP-Adressbereich** und geben Sie dann die erste und letzte IP-Adresse in die Felder **Von IP-Adresse:** und **Bis IP-Adresse:** ein.
6. Alternativ aktivieren Sie **Regel läuft ab in:** und geben die Anzahl an Tagen ein, über die diese Regel erzwungen werden soll.
7. Optional geben Sie eine Beschreibung der Regel ein.
8. Klicken Sie auf **OK**.
9. Klicken Sie im Dialogfeld "Regel für vertrauenswürdige IP-Adresse hinzufügen" auf **Ja**, um die vertrauenswürdige Computerverbindung zu bestätigen.

   Die neu hinzugefügte IP-Adresse wird jetzt im Bereich **Vertrauenswürdige IP-Adressen** angezeigt.

Vertrauenswürdigen Computer aus dem Protokoll "Eingehende Ereignisse" hinzufügen

Sie können eine vertrauenswürdige Computerverbindung und die dazugehörige IP-Adresse aus dem Protokoll "Eingehende Ereignisse" hinzufügen.

Computer mit vertrauenswürdigen IP-Adressen können jederzeit eine Verbindung mit Ihrem Computer herstellen. Bevor Sie eine vertrauenswürdige IP-Adresse hinzufügen, bearbeiten oder entfernen, stellen Sie sicher, dass es sich um eine IP-Adresse handelt, über die eine sichere Kommunikation gewährleistet ist bzw. die sicher entfernt werden kann.

So fügen Sie einen vertrauenswürdigen Computer aus dem Protokoll "Eingehende Ereignisse" hinzu:

1. Stellen Sie sicher, dass das Menü "Erweitert" aktiviert ist. Klicken Sie im Fenster "Häufige Tasks" auf **Berichte & Protokolle**.
2. Klicken Sie unter **Zuletzt aufgetretene Ereignisse** auf **Protokoll anzeigen**.
3. Wählen Sie **Internet & Netzwerk** und anschließend **Eingehende Ereignisse**.
4. Wählen Sie im Bereich "Ausgehende Ereignisse" eine Quell-IP-Adresse aus und klicken Sie dann auf **Diese Adresse als vertrauenswürdig einstufen**.
5. Klicken Sie im Dialogfeld "Regel für vertrauenswürdige IP-Adresse hinzufügen" auf **Ja**, um die vertrauenswürdige IP-Adresse zu bestätigen.

   Die neu hinzugefügte IP-Adresse wird jetzt im Bereich **Vertrauenswürdige IP-Adressen** angezeigt.

Verwandte Themen

- Ereignisprotokollierung (Seite 180)

Vertrauenswürdige Computerverbindung bearbeiten

Sie können eine vertrauenswürdige Computerverbindung und die dazugehörige IP-Adresse bearbeiten.

Computer mit vertrauenswürdigen IP-Adressen können jederzeit eine Verbindung mit Ihrem Computer herstellen. Bevor Sie eine vertrauenswürdige IP-Adresse hinzufügen, bearbeiten oder entfernen, stellen Sie sicher, dass es sich um eine IP-Adresse handelt, über die eine sichere Kommunikation gewährleistet ist bzw. die sicher entfernt werden kann.

So bearbeiten Sie eine vertrauenswürdige Computerverbindung:

1. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" auf die Option **Erweitert**.
2. Klicken Sie im Bereich "Firewall" auf **Vertrauenswürdige und gesperrte IPs**.
3. Wählen Sie im Bereich "Vertrauenswürdige und gesperrte IPs" die Option **Vertrauenswürdige IP-Adressen**.
4. Wählen Sie eine IP-Adresse aus und klicken Sie dann auf **Bearbeiten**.
5. Führen Sie unter **Regel für vertrauenswürdige IP-Adresse** einen der folgenden Schritte aus:
   - Wählen Sie eine **Einzelne IP-Adresse** aus und geben Sie dann die IP-Adresse ein.
   - Wählen Sie einen **IP-Adressbereich** und geben Sie dann die erste und letzte IP-Adresse in die Felder **Von IP-Adresse:** und **Bis IP-Adresse:** ein.
6. Alternativ aktivieren Sie **Regel läuft ab in:** und geben die Anzahl an Tagen ein, über die diese Regel erzwungen werden soll.
7. Optional geben Sie eine Beschreibung der Regel ein.
8. Klicken Sie auf **OK**.

   Die bearbeitete IP-Adresse wird jetzt im Bereich **Vertrauenswürdige IP-Adressen** angezeigt.

Vertrauenswürdige Computerverbindung entfernen

Sie können eine vertrauenswürdige Computerverbindung und die dazugehörige IP-Adresse entfernen.

Computer mit vertrauenswürdigen IP-Adressen können jederzeit eine Verbindung mit Ihrem Computer herstellen. Bevor Sie eine vertrauenswürdige IP-Adresse hinzufügen, bearbeiten oder entfernen, stellen Sie sicher, dass es sich um eine IP-Adresse handelt, über die eine sichere Kommunikation gewährleistet ist bzw. die sicher entfernt werden kann.

So entfernen Sie eine vertrauenswürdige Computerverbindung:

1. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" auf die Option **Erweitert**.
2. Klicken Sie im Bereich "Firewall" auf **Vertrauenswürdige und gesperrte IPs**.
3. Wählen Sie im Bereich "Vertrauenswürdige und gesperrte IPs" die Option **Vertrauenswürdige IP-Adressen**.
4. Wählen Sie eine IP-Adresse aus und klicken Sie dann auf **Entfernen**.
5. Klicken Sie im Dialogfeld **Vertrauenswürdige und gesperrte IPs** auf **Ja**, um das Entfernen der vertrauenswürdigen IP-Adresse unter **Vertrauenswürdige IP-Adressen** zu bestätigen.

Sperren von Computerverbindungen

Sie können vertrauenswürdige IP-Adressen im Bereich "Vertrauenswürdige und gesperrte IPs" unter **Gesperrte IP-Adressen** hinzufügen, bearbeiten und entfernen.

Sie können sicherstellen, dass Computer, die mit unbekannten, verdächtigen oder nicht vertrauenswürdigen IP-Adressen in Verbindung gebracht werden, keine Verbindung zu Ihrem Computer herstellen können.

Da Firewall jeglichen unerwünschten Verkehr blockiert, ist es in der Regel nicht erforderlich, eine IP-Adresse zu sperren. Sie sollten eine IP-Adresse nur dann sperren, wenn Sie sicher sind, dass eine Internetverbindung eine spezifische Bedrohung darstellt. Stellen Sie sicher, dass Sie keine wichtigen IP-Adressen sperren, wie z. B. DNS- bzw. DHCP-Server oder andere Server Ihres ISP. Je nach Ihren Sicherheitseinstellungen kann Firewall Sie benachrichtigen, wenn es ein von einem gesperrten Computer stammendes Ereignis erkennt.

Gesperrte Computerverbindung hinzufügen

Sie können eine gesperrte Computerverbindung und die dazugehörige IP-Adresse hinzufügen.

Sie können sicherstellen, dass Computer, die mit unbekannten, verdächtigen oder nicht vertrauenswürdigen IP-Adressen in Verbindung gebracht werden, keine Verbindung zu Ihrem Computer herstellen können.

Da Firewall jeglichen unerwünschten Verkehr blockiert, ist es in der Regel nicht erforderlich, eine IP-Adresse zu sperren. Sie sollten eine IP-Adresse nur dann sperren, wenn Sie sicher sind, dass eine Internetverbindung eine spezifische Bedrohung darstellt. Stellen Sie sicher, dass Sie keine wichtigen IP-Adressen sperren, wie z. B. DNS- bzw. DHCP-Server oder andere Server Ihres ISP. Je nach Ihren Sicherheitseinstellungen kann Firewall Sie benachrichtigen, wenn es ein von einem gesperrten Computer stammendes Ereignis erkennt.

So fügen Sie eine gesperrte Computerverbindung hinzu:

1. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" auf die Option **Erweitert**.
2. Klicken Sie im Bereich "Firewall" auf **Vertrauenswürdige und gesperrte IPs**.
3. Wählen Sie im Bereich "Vertrauenswürdige und gesperrte IPs" die Option **Gesperrte IP-Adressen** aus.
4. Klicken Sie auf **Hinzufügen**.
5. Führen Sie unter "Regel für vertrauenswürdige IP-Adresse" einen der folgenden Schritte aus:
   - Wählen Sie eine **Einzelne IP-Adresse** aus und geben Sie dann die IP-Adresse ein.
   - Wählen Sie einen **IP-Adressbereich** und geben Sie dann die erste und letzte IP-Adresse in die Felder **Von IP-Adresse:** und **Bis IP-Adresse:** ein.
6. Alternativ aktivieren Sie **Regel läuft ab in:** und geben die Anzahl an Tagen ein, über die diese Regel erzwungen werden soll.
7. Optional geben Sie eine Beschreibung der Regel ein.
8. Klicken Sie auf **OK**.
9. Klicken Sie im Dialogfeld **Regel für vertrauenswürdige IP-Adresse hinzufügen** auf **Ja**, um das Hinzufügen der gesperrten Computerverbindung zu bestätigen.

   Die neu hinzugefügte IP-Adresse wird jetzt im Bereich **Gesperrte IP-Adressen** angezeigt.

Gesperrte Computerverbindung bearbeiten

Sie können eine gesperrte Computerverbindung und die dazugehörige IP-Adresse bearbeiten.

Sie können sicherstellen, dass Computer, die mit unbekannten, verdächtigen oder nicht vertrauenswürdigen IP-Adressen in Verbindung gebracht werden, keine Verbindung zu Ihrem Computer herstellen können.

Da Firewall jeglichen unerwünschten Verkehr blockiert, ist es in der Regel nicht erforderlich, eine IP-Adresse zu sperren. Sie sollten eine IP-Adresse nur dann sperren, wenn Sie sicher sind, dass eine Internetverbindung eine spezifische Bedrohung darstellt. Stellen Sie sicher, dass Sie keine wichtigen IP-Adressen sperren, wie z. B. DNS- bzw. DHCP-Server oder andere Server Ihres ISP. Je nach Ihren Sicherheitseinstellungen kann Firewall Sie benachrichtigen, wenn es ein von einem gesperrten Computer stammendes Ereignis erkennt.

So bearbeiten Sie eine gesperrte Computerverbindung:

1. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" auf die Option **Erweitert**.
2. Klicken Sie im Bereich "Firewall" auf **Vertrauenswürdige und gesperrte IPs**.
3. Wählen Sie im Bereich "Vertrauenswürdige und gesperrte IPs" die Option **Gesperrte IP-Adressen** aus.
4. Wählen Sie eine IP-Adresse aus und klicken Sie dann auf **Bearbeiten**.
5. Führen Sie unter **Regel für vertrauenswürdige IP-Adresse** einen der folgenden Schritte aus:
   - Wählen Sie eine **Einzelne IP-Adresse** aus und geben Sie dann die IP-Adresse ein.
   - Wählen Sie einen **IP-Adressbereich** und geben Sie dann die erste und letzte IP-Adresse in die Felder **Von IP-Adresse:** und **Bis IP-Adresse:** ein.
6. Alternativ aktivieren Sie **Regel läuft ab in:** und geben die Anzahl an Tagen ein, über die diese Regel erzwungen werden soll.
7. Optional geben Sie eine Beschreibung der Regel ein.

   Klicken Sie auf **OK**. Die bearbeitete IP-Adresse wird jetzt im Bereich **Gesperrte IP-Adressen** angezeigt.

Gesperrte Computerverbindung entfernen

Sie können eine gesperrte Computerverbindung und die dazugehörige IP-Adresse entfernen.

Sie können sicherstellen, dass Computer, die mit unbekannten, verdächtigen oder nicht vertrauenswürdigen IP-Adressen in Verbindung gebracht werden, keine Verbindung zu Ihrem Computer herstellen können.

Da Firewall jeglichen unerwünschten Verkehr blockiert, ist es in der Regel nicht erforderlich, eine IP-Adresse zu sperren. Sie sollten eine IP-Adresse nur dann sperren, wenn Sie sicher sind, dass eine Internetverbindung eine spezifische Bedrohung darstellt. Stellen Sie sicher, dass Sie keine wichtigen IP-Adressen sperren, wie z. B. DNS- bzw. DHCP-Server oder andere Server Ihres ISP. Je nach Ihren Sicherheitseinstellungen kann Firewall Sie benachrichtigen, wenn es ein von einem gesperrten Computer stammendes Ereignis erkennt.

So entfernen Sie eine gesperrte Computerverbindung:

1. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" auf die Option **Erweitert**.
2. Klicken Sie im Bereich "Firewall" auf **Vertrauenswürdige und gesperrte IPs**.
3. Wählen Sie im Bereich "Vertrauenswürdige und gesperrte IPs" die Option **Gesperrte IP-Adressen** aus.
4. Wählen Sie eine IP-Adresse aus und klicken Sie auf **Entfernen**.
5. Klicken Sie im Dialogfeld **Vertrauenswürdige und gesperrte IPs** auf **Ja**, um das Entfernen der vertrauenswürdigen IP-Adresse aus **Gesperrte IP-Adressen** zu bestätigen.

Computer aus dem Protokoll "Eingehende Ereignisse" sperren

Sie können eine Computerverbindung und die dazugehörige IP-Adresse aus dem Protokoll "Eingehende Ereignisse" sperren.

IP-Adressen, die in dem Protokoll "Eingehende Ereignisse" aufgeführt sind, sind gesperrt. Folglich stellt das Sperren einer Adresse keinen zusätzlichen Schutz dar, es sei denn, der Computer verfügt über absichtlich geöffnete Ports oder auf Ihrem Computer befindet sich eine Anwendung, der der Zugriff auf eingehende Internetverbindungen gewährt wurde.

Fügen Sie der Liste **Gesperrte IP-Adressen** nur dann eine IP-Adresse hinzu, wenn Sie über mindestens einen absichtlich geöffneten Port verfügen und Sie Grund zu der Annahme haben, dass der Zugriff auf offene Ports von dieser Adresse unterbunden werden muss.

Sie können die Seite "Eingehende Ereignisse", auf der die IP-Adressen des gesamten eingehenden Datenverkehrs aufgeführt werden, dazu verwenden, eine IP-Adresse zu sperren, die vermutlich die Quelle verdächtiger oder unerwünschter Internetaktivität darstellt.

So sperren Sie eine vertrauenswürdige Computerverbindung aus dem Protokoll "Eingehende Ereignisse":

1. Stellen Sie sicher, dass das Menü "Erweitert" aktiviert ist. Klicken Sie im Fenster "Häufige Tasks" auf **Berichte & Protokolle**.
2. Klicken Sie unter **Zuletzt aufgetretene Ereignisse** auf **Protokoll anzeigen**.
3. Wählen Sie **Internet & Netzwerk** und anschließend **Eingehende Ereignisse**.
4. Wählen Sie im Bereich "Eingehende Ereignisse" eine Quell-IP-Adresse aus und klicken Sie dann auf **Diese Adresse sperren**.
5. Klicken Sie im Dialogfeld **Regel für vertrauenswürdige IP-Adresse hinzufügen** auf **Ja**, um das Sperren dieser IP-Adresse zu bestätigen.

   Die neu hinzugefügte IP-Adresse wird jetzt im Bereich **Gesperrte IP-Adressen** angezeigt.

Verwandte Themen

- Ereignisprotokollierung (Seite 180)

Computer aus dem Protokoll "Intrusion Detection-Ereignisse" sperren

Sie können eine Computerverbindung und die dazugehörige IP-Adresse aus dem Protokoll "Intrusion Detection-Ereignisse" sperren.

Sie können sicherstellen, dass Computer, die mit unbekannten, verdächtigen oder nicht vertrauenswürdigen IP-Adressen in Verbindung gebracht werden, keine Verbindung zu Ihrem Computer herstellen können.

Da Firewall jeglichen unerwünschten Verkehr blockiert, ist es in der Regel nicht erforderlich, eine IP-Adresse zu sperren. Sie sollten eine IP-Adresse nur dann sperren, wenn Sie sicher sind, dass eine Internetverbindung eine spezifische Bedrohung darstellt. Stellen Sie sicher, dass Sie keine wichtigen IP-Adressen sperren, wie z. B. DNS- bzw. DHCP-Server oder andere Server Ihres ISP. Je nach Ihren Sicherheitseinstellungen kann Firewall Sie benachrichtigen, wenn es ein von einem gesperrten Computer stammendes Ereignis erkennt.

So sperren Sie einen Computer aus dem Protokoll "Intrusion Detection-Ereignisse":

1. Klicken Sie im Fenster "Häufige Tasks" auf **Berichte & Protokolle**.
2. Klicken Sie unter **Zuletzt aufgetretene Ereignisse** auf **Protokoll anzeigen**.
3. Klicken Sie auf **Internet & Netzwerk** und anschließend auf **Intrusion Detection-Ereignisse**.
4. Wählen Sie im Bereich "Intrusion Detection-Ereignisse" eine Quell-IP-Adresse aus und klicken Sie dann auf **Diese Adresse sperren**.
5. Klicken Sie im Dialogfeld **Regel für vertrauenswürdige IP-Adresse hinzufügen** auf **Ja**, um das Sperren dieser IP-Adresse zu bestätigen.

   Die neu hinzugefügte IP-Adresse wird jetzt im Bereich **Gesperrte IP-Adressen** angezeigt.

Verwandte Themen

- Ereignisprotokollierung (Seite 180)

KAPITEL 23

Protokollierung, Überwachung und Analyse

Firewall bietet umfangreiche und leicht lesbare Protokollierung, Überwachung und Analyse für Internetereignisse und Datenverkehr. Kenntnisse des Internetdatenverkehrs und der -ereignisse helfen Ihnen bei der Verwaltung Ihrer Internetverbindungen.

In diesem Kapitel

Ereignisprotokollierung....180
Mit der Statistik arbeiten....185
Internetverkehr verfolgen....186
Internetdatenverkehr überwachen....191

Ereignisprotokollierung

Mit Firewall können Sie festlegen, ob die Protokollierung aktiviert oder deaktiviert werden soll und welche Ereignistypen protokolliert werden sollen. Mit der Ereignisprotokollierung können Sie vor kurzem aufgetretene eingehende und ausgehende Ereignisse anzeigen. Darüber hinaus können Sie erkannte Intrusionsversuche anzeigen.

Ereignisprotokolleinstellungen konfigurieren

Zur Verfolgung von Firewall-Ereignissen und -Aktivitäten können Sie die anzuzeigenden Ereignistypen festlegen und konfigurieren.

So konfigurieren Sie die Ereignisprotokollierung:

1. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" auf die Option **Erweitert**.
2. Klicken Sie im Bereich "Firewall" auf **Ereignisprotokolleinstellungen**.
3. Führen Sie im Bereich "Ereignisprotokolleinstellungen" einen der folgenden Schritte aus:
   - Wählen Sie **Ereignis protokollieren**, um die Ereignisprotokollierung zu aktivieren.
   - Wählen Sie **Ereignis nicht protokollieren**, um die Ereignisprotokollierung zu deaktivieren.
4. Geben Sie unter **Ereignisprotokolleinstellungen** die zu protokollierenden Ereignistypen an. Die folgenden Typen werden unterstützt:
   - ICMP-Ping-Signale
   - Datenverkehr von gesperrten IP-Adressen
   - Ereignisse an Systemdienstports
   - Ereignisse an unbekannten Ports
   - Ereignisse der Intrusionserkennung (IDS)
5. Wenn Sie die Protokollierung an bestimmten Ports verhindern möchten, wählen Sie **Keine Ereignisse an folgenden Ports protokollieren:** und geben dann die einzelnen Portnummern durch Kommata getrennt bzw. Portbereiche mit Bindestrichen ein. Beispiel: `137-139, 445, 400-5000`.
6. Klicken Sie auf **OK**.

Zuletzt aufgetretene Ereignisse anzeigen

Wenn die Protokollierung aktiviert ist, können Sie die zuletzt aufgetretenen Ereignisse anzeigen. Der Bereich "Zuletzt aufgetretene Ereignisse" zeigt das Datum und eine Beschreibung des Ereignisses an. Der Bereich "Zuletzt aufgetretene Ereignisse" zeigt nur Aktivitäten von Programmen an, deren Zugriff auf das Internet explizit blockiert wurde.

So zeigen Sie die zuletzt aufgetretenen Ereignisse der Firewall an:

- Klicken Sie im Menü **Erweitert** im Bereich "Häufige Tasks" auf **Berichte &Protokolle** oder **Aktuelle Ereignisse anzeigen**. Alternativ können Sie auch auf **Aktuelle Ereignisse anzeigen** im Bereich "Häufige Tasks" des Menüs "Grundlagen" klicken.

Eingehende Ereignisse anzeigen

Wenn die Protokollierung aktiviert ist, können Sie die eingehenden Ereignisse anzeigen und sortieren.

Das Protokoll "Eingehende Ereignisse" enthält die folgenden Protokollkategorien:

- Datum und Uhrzeit
- Quell-IP-Adresse
- Hostname
- Informationen und Ereignistyp

So zeigen Sie die eingehenden Ereignisse der Firewall an:

1. Stellen Sie sicher, dass das Menü "Erweitert" aktiviert ist. Klicken Sie im Fenster "Häufige Tasks" auf **Berichte & Protokolle**.
2. Klicken Sie unter **Zuletzt aufgetretene Ereignisse** auf **Protokoll anzeigen**.
3. Wählen Sie **Internet & Netzwerk** und anschließend **Eingehende Ereignisse**.

Hinweis: Sie können eine IP-Adresse aus dem Protokoll "Eingehende Ereignisse" für vertrauenswürdig erklären, sperren und verfolgen.

Verwandte Themen

- Vertrauenswürdigen Computer aus dem Protokoll "Eingehende Ereignisse" hinzufügen (Seite 170)
- Computer aus dem Protokoll "Eingehende Ereignisse" sperren (Seite 177)
- Computer aus dem Protokoll "Eingehende Ereignisse" verfolgen (Seite 188)

Ausgehende Ereignisse anzeigen

Wenn die Protokollierung aktiviert ist, können Sie die ausgehenden Ereignisse anzeigen. Ausgehende Ereignisse enthalten den Namen des Programms, das einen Zugriff auf eine ausgehende Internetverbindung versucht hat, das Datum und die Uhrzeit des Ereignisses sowie den Speicherort des Programms auf Ihrem Computer.

So zeigen Sie die ausgehenden Ereignisse an:

1. Klicken Sie im Fenster "Häufige Tasks" auf **Berichte & Protokolle**.
2. Klicken Sie unter **Zuletzt aufgetretene Ereignisse** auf **Protokoll anzeigen**.
3. Wählen Sie **Internet & Netzwerk** und anschließend **Ausgehende Ereignisse**.

Hinweis: Die Zugriffsarten "Vollständig" und "Nur ausgehender Zugriff" für ein Programm können Sie auch aus dem Protokoll "Ausgehende Ereignisse" gewähren. Darüber hinaus können Sie weitere Informationen über ein Programm anzeigen.

Verwandte Themen

- Uneingeschränkten Zugriff aus dem Protokoll "Ausgehende Ereignisse" gewähren (Seite 151)
- Nur ausgehenden Zugriff aus dem Protokoll "Ausgehende Ereignisse" gewähren (Seite 154)
- Weitere Programminformationen aus dem Protokoll "Ausgehende Ereignisse" abrufen (Seite 160)

Intrusion Detection-Ereignisse anzeigen

Wenn die Protokollierung aktiviert ist, können Sie die Ereignisse der Intrusionserkennung anzeigen. Intrusion Detection-Ereignisse enthalten das Datum und die Uhrzeit des Ereignisses, die Quell-IP-Adresse und den Hostnamen des Ereignisses. Darüber hinaus beschreibt das Protokoll auch den Ereignistyp.

So zeigen Sie die Intrusion Detection-Ereignisse an:

1. Klicken Sie im Bereich "Häufige Tasks" auf **Berichte & Protokolle**.
2. Klicken Sie unter "Zuletzt aufgetretene Ereignisse" auf **Protokoll anzeigen**.
3. Wählen Sie **Internet & Netzwerk** und klicken Sie dann auf **Intrusion Detection-Ereignisse**.

Hinweis: Sie können eine IP-Adresse aus dem Protokoll "Intrusion Detection-Ereignisse" für vertrauenswürdig erklären, sperren und verfolgen.

Verwandte Themen

- Computer aus dem Protokoll "Intrusion Detection-Ereignisse" sperren (Seite 178)
- Computer aus dem Protokoll "Intrusion Detection-Ereignisse" verfolgen (Seite 189)

Mit der Statistik arbeiten

Die Firewall nutzt die Informationen auf McAfees Hackerwatch-Sicherheitswebsite, um Sie mit Statistiken zu globalen Internet Security-Ereignissen und zur Portaktivität zu versorgen.

Statistiken zu den globalen Sicherheitsereignissen anzeigen

Hackerwatch verfolgt Internet Security-Ereignisse auf der ganzen Welt, die Sie dann im SecurityCenter anzeigen können. Die Informationen umfassen verfolgte Vorfälle, die Hackerwatch während den letzten 24 Stunden, 7 Tagen und 30 Tagen gemeldet wurden.

So zeigen Sie Statistiken zu den globalen Sicherheitsereignissen an:

1. Achten Sie darauf, dass das Menü "Erweitert" aktiviert ist, und klicken Sie dann auf **Extras**.
2. Klicken Sie im Bereich "Extras" auf **Hackerwatch**.
3. Zeigen Sie die Statistiken zu den Sicherheitsereignissen unter **Ereignisverfolgung** an.

Globale Portaktivität anzeigen

Hackerwatch verfolgt Internet Security-Ereignisse auf der ganzen Welt, die Sie dann im SecurityCenter anzeigen können. Die angezeigten Informationen umfassen die wichtigsten Ports, die Hackerwatch während der letzten sieben Tage gemeldet wurden. In der Regel werden hier HTTP-, TCP-, und UDP-Portinformationen angezeigt.

So zeigen Sie die weltweite Portaktivität an:

1. Achten Sie darauf, dass das Menü "Erweitert" aktiviert ist, und klicken Sie dann auf **Extras**.
2. Klicken Sie im Bereich "Extras" auf **Hackerwatch**.
3. Zeigen Sie die wichtigsten Ports unter **Recent Port Activity** an.

Internetverkehr verfolgen

Die Firewall bietet Ihnen verschiedene Optionen zur Verfolgung des Internet-Datenverkehrs. Mit diesen Optionen können Sie einen Netzwerkcomputer geografisch (auf einer Weltkarte) verfolgen, Domänen- und Netzwerkinformationen erhalten und Computer aus den Protokollen "Eingehende Ereignisse" und "Intrusion Detection-Ereignisse" verfolgen.

So verfolgen Sie einen Netzwerkcomputer geografisch:

Mit Visual Tracer können Sie einen Computer, der eine Verbindung mit Ihrem Computer hergestellt hat oder herzustellen versucht, anhand seines Namens oder seiner IP-Adresse geografisch lokalisieren. Darüber hinaus können Sie mit Visual Tracer auch Informationen zum Netzwerk und den Registrierungsinformationen erhalten. Nach dem Aufrufen von Visual Tracer wird eine Weltkarte mit der wahrscheinlichsten Datenroute zwischen dem Quellcomputer und Ihrem Computer angezeigt.

So lokalisieren Sie einen Computer geografisch:

1. Achten Sie darauf, dass das Menü "Erweitert" aktiviert ist, und klicken Sie dann auf **Extras**.
2. Klicken Sie im Bereich "Extras" auf **Visual Tracer**.
3. Geben Sie die IP-Adresse des Computers ein und klicken Sie auf **Ablaufverfolgung**.
4. Wählen Sie unter **Visual Tracer** die Option **Kartenansicht**.

Hinweis: Private, ungültige oder Looped-IP-Adressen können Sie nicht verfolgen.

Registrierungsinformationen eines Computers erhalten

Mithilfe von Visual Tracer können Sie die Registrierungsinformationen eines Computers von SecurityCenter erhalten. Die Registrierungsinformationen enthalten den Namen der Domäne, den Namen des Registranten mit Adresse sowie administrative Kontaktinformationen.

So erhalten Sie Informationen zur Domäne eines Computers:

1. Achten Sie darauf, dass das Menü "Erweitert" aktiviert ist, und klicken Sie dann auf **Extras**.
2. Klicken Sie im Bereich "Extras" auf **Visual Tracer**.
3. Geben Sie die IP-Adresse des Computers ein und klicken Sie auf **Ablaufverfolgung**.
4. Wählen Sie unter **Visual Tracer** die Option **Registrant-Ansicht**.

Netzwerkinformationen eines Computers erhalten

Mithilfe von Visual Tracer können Sie die Netzwerkinformationen eines Computers von SecurityCenter erhalten. Die Netzwerkinformationen enthalten Details über das Netzwerk, in dem sich die Domäne befindet.

So erhalten Sie die Netzwerkinformationen eines Computers:

1. Achten Sie darauf, dass das Menü "Erweitert" aktiviert ist, und klicken Sie dann auf **Extras**.
2. Klicken Sie im Bereich "Extras" auf **Visual Tracer**.
3. Geben Sie die IP-Adresse des Computers ein und klicken Sie auf **Ablaufverfolgung**.
4. Wählen Sie unter **Visual Tracer** die Option **Netzwerkansicht**.

Computer aus dem Protokoll "Eingehende Ereignisse" verfolgen

In dem Bereich "Eingehende Ereignisse" können Sie eine IP-Adresse verfolgen, die im Protokoll "Eingehende Ereignisse" aufgeführt wird.

So verfolgen Sie die IP-Adresse eines Computers aus dem Protokoll "Eingehende Ereignisse":

1. Stellen Sie sicher, dass das Menü "Erweitert" aktiviert ist. Klicken Sie im Fenster "Häufige Tasks" auf **Berichte & Protokolle**.
2. Klicken Sie unter **Zuletzt aufgetretene Ereignisse** auf **Protokoll anzeigen**.
3. Wählen Sie **Internet & Netzwerk** und anschließend **Eingehende Ereignisse**.
4. Wählen Sie im Bereich "Eingehende Ereignisse" eine Quell-IP-Adresse aus und klicken Sie dann auf **Diese Adresse verfolgen**.
5. Wählen Sie im Bereich "Visual Tracer" eine der folgenden Optionen aus:
   - **Kartenansicht**: Lokalisieren Sie einen Computer geografisch anhand der ausgewählten IP-Adresse.
   - **Registrant-Ansicht**: Lokalisieren Sie die Domäneninformationen anhand der ausgewählten IP-Adresse.
   - **Netzwerkansicht**: Lokalisieren Sie die Netzwerkinformationen anhand der ausgewählten IP-Adresse.
6. Klicken Sie auf **Fertig**.

Verwandte Themen

- Internetverkehr verfolgen (Seite 186)
- Eingehende Ereignisse anzeigen (Seite 182)

Computer aus dem Protokoll "Intrusion Detection-Ereignisse" verfolgen

In dem Bereich "Intrusion Detection-Ereignisse" können Sie eine IP-Adresse verfolgen, die im Protokoll "Intrusion Detection-Ereignisse" aufgeführt wird.

So verfolgen Sie die IP-Adresse eines Computers aus dem Protokoll "Intrusion Detection-Ereignisse":

1. Klicken Sie im Fenster "Häufige Tasks" auf **Berichte & Protokolle**.
2. Klicken Sie unter **Zuletzt aufgetretene Ereignisse** auf **Protokoll anzeigen**.
3. Klicken Sie auf **Internet & Netzwerk** und anschließend auf **Intrusion Detection-Ereignisse**.Wählen Sie im Bereich "Intrusion Detection-Ereignisse" eine Quell-IP-Adresse aus und klicken Sie dann auf **Diese Adresse verfolgen**.
4. Wählen Sie im Bereich "Visual Tracer" eine der folgenden Optionen aus:
   - **Kartenansicht**: Lokalisieren Sie einen Computer geografisch anhand der ausgewählten IP-Adresse.
   - **Registrant-Ansicht**: Lokalisieren Sie die Domäneninformationen anhand der ausgewählten IP-Adresse.
   - **Netzwerkansicht**: Lokalisieren Sie die Netzwerkinformationen anhand der ausgewählten IP-Adresse.
5. Klicken Sie auf **Fertig**.

Verwandte Themen

- Internetverkehr verfolgen (Seite 186)
- Protokollierung, Überwachung und Analyse (Seite 179)

Überwachte IP-Adresse verfolgen

Sie können eine überwachte IP-Adresse verfolgen. Dazu wird eine Weltkarte aufgerufen, die die wahrscheinlichste Datenroute zwischen dem Quellcomputer und Ihrem Computer anzeigt. Darüber hinaus können Sie die Registrierungs- und Netzwerkinformationen zu dieser IP-Adresse in Erfahrung bringen.

So überwachen Sie die verwendete Programmbandbreite:

1. Achten Sie darauf, dass das Menü "Erweitert" aktiviert ist, und klicken Sie auf **Extras**.
2. Klicken Sie im Bereich "Extras" auf **Datenverkehrsmonitor**.
3. Klicken Sie unter **Datenverkehrsmonitor** auf **Aktive Programme**.
4. Wählen Sie ein Programm und dann die IP-Adresse aus, die unterhalb des Programmnamens angezeigt wird.
5. Aktivieren Sie unter **Programmaktivität** die Option **Diese IP verfolgen**.
6. Unter **Visual Tracer** wird eine Weltkarte mit der wahrscheinlichsten Datenroute zwischen dem Quellcomputer und Ihrem Computer angezeigt. Darüber hinaus können Sie die Registrierungs- und Netzwerkinformationen zu dieser IP-Adresse in Erfahrung bringen.

Hinweis: Um die aktuellen Statistiken anzuzeigen, klicken Sie unter **Visual Tracer** auf **Aktualisieren**.

Verwandte Themen

- Internetdatenverkehr überwachen (Seite 191)

Internetdatenverkehr überwachen

Die Firewall bietet verschiedene Methoden zur Überwachung des Internetdatenverkehrs an:

- **Diagramm "Datenverkehrsanalyse"**: Zeigt die zuletzt registrierten eingehenden und ausgehenden Internetverbindungen an.
- **Diagramm "Datenverkehrsverwendung"**: Zeigt den Prozentsatz der Bandbreite an, der in den vergangenen 24 Stunden von den Anwendungen mit der höchsten Aktivität verwendet wurde.
- **Aktive Programme**: Zeigt die Anwendungen an, die momentan die meisten Netzwerkverbindungen auf dem Computer verwenden, sowie die IP-Adressen, auf die diese Anwendungen zugreifen.

Info zum Diagramm "Datenverkehrsanalyse"

Das Diagramm "Datenverkehrsanalyse" ist eine numerische und graphische Darstellung des ein- und abgehenden Internet-Datenverkehrs. Der Datenverkehrsmonitor zeigt zudem Programme an, die die höchste Anzahl an Netzwerkverbindungen auf Ihrem Computer verwenden, sowie die IP-Adressen, auf die die Programme zugreifen.

In dem Bereich "Datenverkehrsanalyse" können Sie den zuletzt registrierten eingehenden und ausgehenden Internetdatenverkehr sowie die aktuellen, mittleren und maximal Übertragungsraten anzeigen. Darüber hinaus können Sie den Datenverkehr anzeigen, einschließlich des gemessenen Datenverkehrs seit dem Start der Firewall und des gesamten Datenverkehrs für den aktuellen und die vorherigen Monate.

Im Bereich "Datenverkehrsanalyse" wird die Echtzeit-Internetaktivität auf Ihrem Computer angezeigt, einschließlich der Datenmenge und Übertragungsrate von zuletzt registriertem eingehenden und ausgehenden Internetdatenverkehr auf Ihrem Computer, der Verbindungsgeschwindigkeit und der Gesamtzahl an Bytes, die über das Internet übertragen wurden.

Die durchgezogene grüne Linie stellt die aktuelle Übertragungsrate für eingehenden Datenverkehr dar. Die gepunktete grüne Linie stellt die durchschnittliche Übertragungsrate für eingehenden Datenverkehr dar. Wenn die aktuelle und die durchschnittliche Übertragungsrate identisch sind, wird die gepunktete Linie im Diagramm nicht angezeigt. Die durchgezogene Linie stellt sowohl die durchschnittliche als auch die aktuelle Übertragungsrate dar.

Die durchgezogene rote Linie stellt die aktuelle Übertragungsrate für ausgehenden Datenverkehr dar. Die gepunktete rote Linie stellt die durchschnittliche Übertragungsrate für ausgehenden Datenverkehr dar. Wenn die aktuelle und die durchschnittliche Übertragungsrate identisch sind, wird die gepunktete Linie im Diagramm nicht angezeigt. Die durchgezogene Linie stellt sowohl die durchschnittliche als auch die aktuelle Übertragungsrate dar.

Verwandte Themen

- Eingehenden und ausgehenden Datenverkehr analysieren (Seite 193)

Eingehenden und ausgehenden Datenverkehr analysieren

Das Diagramm "Datenverkehrsanalyse" ist eine numerische und graphische Darstellung des ein- und abgehenden Internet-Datenverkehrs. Der Datenverkehrsmonitor zeigt zudem Programme an, die die höchste Anzahl an Netzwerkverbindungen auf Ihrem Computer verwenden, sowie die IP-Adressen, auf die die Programme zugreifen.

So analysieren Sie den eingehenden und ausgehenden Datenverkehr:

1. Achten Sie darauf, dass das Menü "Erweitert" aktiviert ist, und klicken Sie dann auf **Extras**.
2. Klicken Sie im Bereich "Extras" auf **Datenverkehrsmonitor**.
3. Klicken Sie unter **Datenverkehrsmonitor** auf **Datenverkehrsanalyse**.

Tipp: Um die aktuellen Statistiken anzuzeigen, klicken Sie unter **Datenverkehrsanalyse** auf **Aktualisieren**.

Verwandte Themen

- Info zum Diagramm "Datenverkehrsanalyse" (Seite 192)

Programmbandbreite überwachen

Sie können ein Kreisdiagramm anzeigen, in dem der ungefähre Prozentsatz der Bandbreite dargestellt wird, der in den vergangenen 24 Stunden von den Anwendungen mit der höchsten Aktivität verwendet wurde. Das Kreisdiagramm dient der visuellen Darstellung der relativen Bandbreite, die von den Programmen genutzt wird.

So überwachen Sie die verwendete Programmbandbreite:

1. Achten Sie darauf, dass das Menü "Erweitert" aktiviert ist, und klicken Sie dann auf **Extras**.
2. Klicken Sie im Bereich "Extras" auf **Datenverkehrsmonitor**.
3. Klicken Sie unter **Datenverkehrsmonitor** auf **Datenverkehrsverwendung**.

Tipp: Um die aktuellen Statistiken anzuzeigen, klicken Sie unter **Datenverkehrsverwendung** auf **Aktualisieren**.

Programmaktivität überwachen

Sie können die eingehende und ausgehende Programmaktivität anzeigen, in der die Remote-Computerverbindungen und -ports enthalten sind.

So überwachen Sie die verwendete Programmbandbreite:

1. Achten Sie darauf, dass das Menü "Erweitert" aktiviert ist, und klicken Sie dann auf **Extras**.
2. Klicken Sie im Bereich "Extras" auf **Datenverkehrsmonitor**.
3. Klicken Sie unter **Datenverkehrsmonitor** auf **Aktive Programme**.
4. Sie können die folgenden Informationen anzeigen:
   - Diagramm "Programmaktivität": Wählen Sie ein Programm, um dessen Aktivität in Diagrammform darzustellen.
   - Überwachungsverbindung: Wählen Sie ein Überwachungselement unter dem Programmnamen.
   - Computerverbindung: Wählen Sie eine IP-Adresse unter dem Programmnamen, Systemprozess oder Dienst.

Hinweis: Um die aktuellen Statistiken anzuzeigen, klicken Sie unter **Aktive Programme** auf **Aktualisieren**.

KAPITEL 24

Weitere Informationen zu Internet Security

Die Firewall nutzt die Informationen auf McAfees Sicherheitswebsite Hackerwatch, um Ihnen aktuelle Informationen zu Programmen und der globalen Internetaktivität bereitzustellen. Außerdem bietet Hackerwatch ein HTML-Lernprogramm für die Firewall.

In diesem Kapitel

Hackerwatch-Lernprogramm starten.....196

Hackerwatch-Lernprogramm starten

Wissenswertes zur Firewall finden Sie im Hackerwatch-Lernprogramm von SecurityCenter.

So starten Sie das Hackerwatch-Lernprogramm:

1. Achten Sie darauf, dass das Menü "Erweitert" aktiviert ist, und klicken Sie dann auf **Extras**.
2. Klicken Sie im Bereich "Extras" auf **Hackerwatch**.
3. Klicken Sie unter **Hackerwatch-Ressourcen** auf **Lernprogramm anzeigen**.

KAPITEL 25

McAfee SpamKiller

SpamKiller filtert Spam- und Phishing-E-Mails und bietet folgendes:

Benutzeroptionen

- Filtern mehrerer E-Mail-Konten
- Importieren von Kontakten in die Freunde-Liste
- Erstellen benutzerdefinierter Filter und Einsenden von Spam an McAfee zur Analyse
- Optionen "Als Spam markieren" und "Nicht als Spam markieren"
- Unterstützt mehrere Benutzer (Windows(R) XP und Vista™)

Filtern

- Automatisches Aktualisieren von Filtern
- Erstellen benutzerdefinierter E-Mail-Filter
- Mehrstufiges Kernfiltermodul
- Phishing-Filter

In diesem Kapitel

Funktionen 198
Verwalten von Web-Mail-Konten 201
Verwalten von Freunden 209
Ändern von Filteroptionen 215
Verwalten persönlicher Filter 221
Verwalten von SpamKiller 231
Konfigurieren des Phishing-Schutzes.....235
Zusätzliche Hilfe.....239

Funktionen

Diese Version von SpamKiller umfasst folgende neue Funktionen:

Filtern

Die erweiterte Filter-Technologie macht die Benutzung angenehmer.

Phishing

Mittels der Funktion "Phishing" können potentielle Phishing-Websites identifiziert und blockiert werden.

Installation

Setup und Konfiguration wurden vereinfacht.

Benutzeroberfläche

Eine intuitive Benutzeroberfläche unterstützt Sie dabei, Spam von Ihrem Computer fernzuhalten.

Support

Kostenloser technischer Support per Instant Messaging und E-Mail ermöglicht einen unkomplizierten, sofortigen und direkten Kundendienst.

Verarbeitung von Spam-Nachrichten

Optionale Einstellungen für die Bearbeitung von Spam-E-Mails. So können Sie Nachrichten anzeigen, die möglicherweise inkorrekt gefiltert wurden.

Unterstützte E-Mail-Programme

- Jedes POP3-E-Mail-Programm
- MAPI-Unterstützung für Outlook(R) 2000 oder höher
- Filter-Unterstützung für Web-Mail über POP3 oder kostenpflichtiges MSN(R)/Hotmail(R)

Unterstützte E-Mail-Symbolleisten

- Outlook Express 6.0 oder höher
- Outlook 2000, XP, 2003 oder 2007
- Eudora(R) 6.0 oder höher
- Thunderbird™ 1.5 oder höher

Unterstützter Phishing-Schutz

Alle HTTP-kompatiblen Web-Browser, einschließlich:

- Internet Explorer
- Firefox(R)
- Netscape(R)

KAPITEL 26

Verwalten von Web-Mail-Konten

Sie können Web-Mail-Konten hinzufügen, um Spam zu filtern, Web-Mail-Kontoinformationen zu bearbeiten oder um Web-Mail-Konten zu entfernen, wenn diese nicht mehr benötigt werden.

Außerdem haben Sie die Möglichkeit, das Web-Mail-Filtern zu verwalten. Sie können beispielsweise das Filtern von E-Mail-Nachrichten in Ihren Web-Mail-Konten deaktivieren oder aktivieren, gefilterte Nachrichten verwalten und Protokolle anzeigen.

In diesem Kapitel

Hinzufügen von Web-Mail-Konten 202
Ändern von Web-Mail-Konten.....204
Entfernen von Web-Mail-Konten 206
Verwalten der Filterung von Web-Mail-Konten 207

Hinzufügen von Web-Mail-Konten

Sie können die folgenden Typen von Web-Mail-Konten hinzufügen, so dass Spam heraus gefiltert werden kann.

- POP3-Web-Mail (z. B. Yahoo®)
- MSN/Hotmail (es werden nur bezahlte Versionen voll unterstützt)

Hinzufügen eines POP3- oder MSN/Hotmail-Web-Mail-Kontos

Fügen Sie ein E-Mail-Konto hinzu, damit dieses nach Spam gefiltert wird.

So fügen Sie ein POP3- oder MSN/Hotmail-Web-Mail-Konto hinzu:

1. Klicken Sie im Menü "Erweitert" auf **Konfigurieren**.
2. Klicken Sie im Konfigurationsbereich auf **E-Mail & IM**.
3. Klicken Sie unter **Spam-Schutz** auf **Erweitert**.
4. Klicken Sie im Bereich "Spam-Schutz" auf **Web-Mail-Konten**.
5. Klicken Sie im Bereich "Web-Mail-Konten" auf **Hinzufügen**.
6. Geben Sie die Informationen des Web-Mail-Kontos in die folgenden Felder ein:
   - **Beschreibung** - Beschreibt das Konto. Sie können beliebige Informationen in dieses Feld eingeben.
   - **E-Mail-Adresse**: Gibt die E-Mail-Adresse dieses Kontos an.
   - **Kontotyp**: Gibt den Typ eines E-Mail-Kontos an.
   - **Server**: Gibt den Namen des Servers für dieses Konto an.
   - **Benutzername**: Gibt den Benutzernamen für dieses Konto an.
   - **Kennwort**: Gibt das Kennwort für den Zugriff auf dieses Konto an.
   - **Kennwort bestätigen**: Bestätigt das Kennwort.
7. Klicken Sie auf **Weiter**.
8. Führen Sie unter **Überprüfungsoptionen** eine der folgenden Aktionen durch, um festzulegen, wann SpamKiller Ihr Konto auf Spam überprüft:
   - Geben Sie im Feld **Überprüfen alle** einen Wert ein.

SpamKiller überprüft dieses Konto im angegebenen Intervall (Anzahl Minuten). Wenn Sie eine Null eingeben, überprüft SpamKiller das Konto nur beim Herstellen einer Verbindung.

- Aktivieren Sie das Kontrollkästchen **Beim Starten prüfen**.

  SpamKiller überprüft das Konto jedes Mal, wenn Sie den Computer neu starten. Verwenden Sie diese Option, wenn Ihr Computer über eine Direktverbindung verfügt.

9 Wenn Sie eine Einwahlverbindung verwenden, führen Sie einen der folgenden Schritte unter **Verbindungsoptionen** aus, um festzulegen, wie SpamKiller eine Verbindung mit dem Internet herstellt:

- Klicken Sie auf **Nie eine Einwahlverbindung herstellen.**

  SpamKiller stellt nicht automatisch eine Einwahlverbindung her. Sie müssen Ihre Einwahlverbindung zuerst manuell starten, bevor SpamKiller in Aktion treten kann.

- Klicken Sie auf **Einwählen, wenn keine Verbindung verfügbar ist**.

  Wenn keine Internetverbindung vorhanden ist, versucht SpamKiller automatisch, unter Verwendung der von Ihnen angegebenen Einwahlverbindung eine Verbindung herzustellen.

- Klicken Sie auf **Immer mit der angegebenen Verbindung einwählen**.

  SpamKiller versucht unter Verwendung der angegebenen Einwahlverbindung eine Verbindung herzustellen.

- Klicken Sie auf einen Eintrag in der Liste **Mit dieser Verbindung einwählen**.

  Dieser Eintrag bestimmt die Einwahlverbindung, über die SpamKiller versucht, eine Verbindung herzustellen.

- Aktivieren Sie das Kontrollkästchen **Verbindung beibehalten, nachdem die Filterung abgeschlossen wurde**.

  Ihr Computer bleibt mit dem Internet verbunden, nachdem der Filtervorgang abgeschlossen wurde.

10 Klicken Sie auf **Fertig stellen**.

Ändern von Web-Mail-Konten

Sie können Web-Mail-Konten aktivieren, deaktivieren oder deren Informationen bearbeiten. Sie können beispielsweise die E-Mail-Adresse, die Kontobeschreibung, den Kontotyp, das Kennwort, die Häufigkeit der Überprüfungen des Kontos auf Spam und die Art der Internetverbindung ändern.

Bearbeiten eines POP3- oder MSN/Hotmail-Web-Mail-Kontos

Sie können Web-Mail-Konten aktivieren oder deaktivieren sowie ihre Informationen bearbeiten. Dazu gehören beispielsweise die E-Mail-Adresse, die Kontobeschreibung, die Serverinformationen, die Häufigkeit der Überprüfungen des Kontos auf Spam und die Art der Internetverbindung.

So bearbeiten Sie ein POP3- oder MSN/Hotmail-Web-Mail-Konto:

1. Klicken Sie im Menü "Erweitert" auf **Konfigurieren**.
2. Klicken Sie im Konfigurationsbereich auf **E-Mail & IM**.
3. Klicken Sie unter **Spam-Schutz** auf **Erweitert**.
4. Klicken Sie im Bereich "Spam-Schutz" auf **Web-Mail-Konten**.
5. Wählen Sie das Konto aus, das bearbeitet werden soll, und klicken Sie dann auf **Bearbeiten**.
6. Geben Sie die Kontoinformationen in die folgenden Felder ein:
   - **Beschreibung** - Beschreibt das Konto. Sie können beliebige Informationen in dieses Feld eingeben.
   - **E-Mail-Adresse**: Gibt die E-Mail-Adresse dieses Kontos an.
   - **Kontotyp**: Gibt den Typ eines E-Mail-Kontos an.
   - **Server**: Gibt den Namen des Servers für dieses Konto an.
   - **Benutzername**: Gibt den Benutzernamen für dieses Konto an.
   - **Kennwort**: Gibt das Kennwort für den Zugriff auf dieses Konto an.
   - **Kennwort bestätigen**: Bestätigt das Kennwort.
7. Klicken Sie auf **Weiter**.
8. Führen Sie unter **Überprüfungsoptionen** eine der folgenden Aktionen durch, um festzulegen, wann SpamKiller Ihr Konto auf Spam überprüft:
   - Geben Sie im Feld **Überprüfen alle** einen Wert ein.

SpamKiller überprüft dieses Konto im angegebenen Intervall (Anzahl Minuten). Wenn Sie eine Null eingeben, überprüft SpamKiller das Konto nur beim Herstellen einer Verbindung.

- Aktivieren Sie das Kontrollkästchen **Beim Starten prüfen**.

  SpamKiller überprüft das Konto jedes Mal, wenn Sie den Computer neu starten. Verwenden Sie diese Option, wenn Ihr Computer über eine Direktverbindung verfügt.

9 Wenn Sie eine Einwahlverbindung verwenden, führen Sie einen der folgenden Schritte unter **Verbindungsoptionen** aus, um festzulegen, wie SpamKiller eine Verbindung mit dem Internet herstellt:

- Klicken Sie auf **Nie eine Einwahlverbindung herstellen.**

  SpamKiller stellt nicht automatisch eine Einwahlverbindung her. Sie müssen Ihre Einwahlverbindung zuerst manuell starten, bevor SpamKiller in Aktion treten kann.

- Klicken Sie auf **Einwählen, wenn keine Verbindung verfügbar ist**.

  Wenn keine Internetverbindung vorhanden ist, versucht SpamKiller automatisch, unter Verwendung der von Ihnen angegebenen Einwahlverbindung eine Verbindung herzustellen.

- Klicken Sie auf **Immer mit der angegebenen Verbindung einwählen**.

  SpamKiller versucht unter Verwendung der angegebenen Einwahlverbindung eine Verbindung herzustellen.

- Klicken Sie auf einen Eintrag in der Liste **Mit dieser Verbindung einwählen**.

  Dieser Eintrag bestimmt die Einwahlverbindung, über die SpamKiller versucht, eine Verbindung herzustellen.

- Aktivieren Sie das Kontrollkästchen **Verbindung beibehalten, nachdem die Filterung abgeschlossen wurde**.

  Ihr Computer bleibt mit dem Internet verbunden, nachdem der Filtervorgang abgeschlossen wurde.

10 Klicken Sie auf **Fertig stellen**.

Entfernen von Web-Mail-Konten

Sie können Web-Mail-Konten, die nicht länger gefiltert werden sollen, entfernen.

Entfernen von Web-Mail-Konten

Wenn Sie möchten, dass ein E-Mail-Konto nicht mehr gefiltert wird, entfernen Sie das entsprechende Konto.

So entfernen Sie Web-Mail-Konten:

1. Klicken Sie im Menü "Erweitert" auf **Konfigurieren**.
2. Klicken Sie im Fenster "Konfigurieren" auf **E-Mail & IM**.
3. Klicken Sie unter **Spam-Schutz** auf **Erweitert**.
4. Klicken Sie im Fenster "Spam-Schutz" auf **Web Mail AccountsWeb-Mail-Konten**.
5. Wählen Sie das zu entfernenden Konto aus und klicken Sie dann auf **Entfernen**.

Verwalten der Filterung von Web-Mail-Konten

Sie können das Filtern von E-Mail-Nachrichten in Ihren Web-Mail-Konten deaktivieren oder aktivieren, gefilterte Nachrichten verwalten und Protokolle anzeigen.

Deaktivieren der Filterung von Web-Mail-Konten

Sie können das Filtern von Web-Mail deaktivieren, so dass E-Mail-Nachrichten nicht gefiltert werden.

So deaktivieren Sie das Filtern von Web-Mail-Konten:

1. Klicken Sie im Menü "Erweitert" auf **Konfigurieren**.
2. Klicken Sie im Fenster "Konfigurieren" auf **E-Mail & IM**.
3. Klicken Sie unter **Spam-Schutz** auf **Erweitert**.
4. Klicken Sie im Fenster "Spam-Schutz" auf **Web Mail AccountsWeb-Mail-Konten**.
5. Aktivieren Sie das Kontrollkästchen neben dem Konto, das deaktiviert werden soll.
6. Klicken Sie auf **OK**.

Aktiveren der Filterung von Web-Mail-Konten

Sie können deaktivierte Web-Mail-Konten auch wieder aktivieren.

So aktivieren Sie das Filtern von Web-Mail-Konten:

1. Klicken Sie im Menü "Erweitert" auf **Konfigurieren**.
2. Klicken Sie im Fenster "Konfigurieren" auf **E-Mail & IM**.
3. Klicken Sie unter **Spam-Schutz** auf **Erweitert**.
4. Klicken Sie im Fenster "Spam-Schutz" auf **Web Mail AccountsWeb-Mail-Konten**.
5. Aktivieren Sie das Kontrollkästchen neben dem Konto, das aktiviert werden soll.
6. Klicken Sie auf **OK**.

Verwalten von gefilterten Nachrichten in Web-Mail-Konten

Sie können Nachrichten, die in Ihrem Web-Mail-Konto gefiltert wurden, anzeigen, kopieren oder löschen.

So zeigen Sie gefilterte Nachrichten für Ihr Web-Mail-Konto an oder kopieren oder löschen diese:

1. Klicken Sie im Menü "Erweitert" auf **Berichte & Protokolle**.
2. Klicken Sie im Fenster "Berichte & Protokolle" auf **Gefilterte Web-Mails**.
3. Wählen Sie im Fenster "Gefilterte Web-Mails" die Nachricht aus, die Sie anzeigen, kopieren oder löschen möchten.
4. Führen Sie unter **Ich möchte** einen der folgenden Schritte aus:
   - Klicken Sie auf **Kopieren**, um die Nachricht in die Zwischenablage zu kopieren.
   - Klicken Sie auf **Löschen**, um die Nachricht zu löschen.

Anzeigen von Protokollen für gefilterte Web-Mail

Sie können Protokolle für gefilterte Web-Mail anzeigen. Sie können beispielsweise anzeigen, wann die E-Mail-Nachricht gefiltert wurde, und das Konto, in dem sie eingegangen ist.

So zeigen Sie Protokolle für gefilterte Web-Mail an:

1. Klicken Sie im Menü "Erweitert" auf **Berichte & Protokolle**.
2. Klicken Sie im Fenster "Berichte & Protokolle" auf **Zuletzt aufgetretene Ereignisse**.
3. Klicken Sie im Fenster "Zuletzt aufgetretene Ereignisse" auf **Protokoll anzeigen**.
4. Erweitern Sie im linken Fenster die Liste **E-Mail & IM** und klicken Sie anschließend auf **Web-Mail-Filterereignisse**.
5. Wählen Sie das Protokoll aus, das Sie sich ansehen möchten.
6. Lesen Sie unter **Details** die Informationen zu diesem Protokoll.

KAPITEL 27

Verwalten von Freunden

Nehmen Sie die Adressen Ihrer Freunde in eine Freunde-Liste auf, damit gewährleistet ist, dass alle E-Mails dieser Personen wirklich bei Ihnen eingehen. Sie können auch Domänen hinzufügen, Freunde bearbeiten oder entfernen und automatische Aktualisierungen der Freunde-Liste planen.

In diesem Kapitel

Grundlegendes zum Verwalten von Freunden 210
Automatisches Aktualisieren von Freunden 212

Grundlegendes zum Verwalten von Freunden

In diesem Abschnitt wird beschrieben, wie Sie Freunde verwalten.

Manuelles Hinzufügen von Freunden in der SpamKiller-Symbolleiste

Um sicherzugehen, dass Sie alle Nachrichten von Freunden erhalten, sollten Sie ihre Adressen zu Ihrer Freunde-Liste hinzufügen.

Wenn Sie eines der E-Mail-Programme Outlook, Outlook Express, Windows Mail, Eudora oder Thunderbird verwenden, können Sie über die SpamKiller-Symbolleiste Freunde hinzufügen.

So fügen Sie einen Freund von Outlook aus hinzu:

- Wählen Sie in Ihrem E-Mail-Programm eine Nachricht aus und klicken Sie auf **Freund hinzufügen**.

So fügen Sie einen Freund von Outlook Express, Windows Mail, Eudora oder Thunderbird aus hinzu:

- Wählen Sie in Ihrem E-Mail-Programm eine Nachricht aus. Klicken Sie dann im Menü **SpamKiller** auf **Freund hinzufügen**.

Manuelles Hinzufügen von Freunden

Nehmen Sie die Adressen Ihrer Freunde in eine Freunde-Liste auf, damit gewährleistet ist, dass alle E-Mails von diesen Personen wirklich bei Ihnen eingehen. Sie können auch Domänen hinzufügen.

So fügen Sie Freunde manuell hinzu:

1. Klicken Sie im Menü "Erweitert" auf **Konfigurieren**.
2. Klicken Sie im Fenster "Konfigurieren" auf **E-Mail & IM**.
3. Klicken sie unter "Spam-Schutz" auf **Erweitert**.
4. Klicken Sie im Fenster "Spam-Schutz" auf **Freunde**.
5. Klicken Sie im Fenster "Freunde" auf **Hinzufügen**.
6. Geben Sie die Informationen zu Ihrem Freund in die folgenden Felder ein:
   - **Name**: Gibt den Namen des Freundes an.
   - **Typ**: Gibt an, ob Sie eine einzelne E-Mail-Adresse oder eine gesamte Domäne angeben.
   - **E-Mail-Adresse**: Gibt die E-Mail-Adresse des Freundes oder die Domäne an, die nicht gefiltert werden soll.
7. Klicken Sie auf **OK**.

Bearbeiten von Freunden

Wenn sich die Informationen zu einem Freund ändern, können Sie die Liste aktualisieren, um sicherzustellen, dass Sie alle Nachrichten von dieser Person empfangen.

So bearbeiten Sie Freunde:

1. Klicken Sie im Menü "Erweitert" auf **Konfigurieren**.
2. Klicken Sie im Fenster "Konfigurieren" auf **E-Mail & IM**.
3. Klicken sie unter "Spam-Schutz" auf **Erweitert**.
4. Klicken Sie im Fenster "Spam-Schutz" auf **Freunde**.
5. Wählen Sie den zu bearbeitenden Freund aus und klicken Sie anschließend auf **Bearbeiten**.
6. Bearbeiten Sie die Informationen zu Ihrem Freund in folgenden Feldern:
   - **Name**: Gibt den Namen des Freundes an.
   - **Typ**: Gibt an, ob Sie eine einzelne E-Mail-Adresse oder eine gesamte Domäne bearbeiten.
   - **E-Mail-Adresse**: Gibt die E-Mail-Adresse des Freundes oder die Domäne an, die nicht gefiltert werden soll.
7. Klicken Sie auf **OK**.

Entfernen von Freunden

Entfernen Sie Freunde von dieser Liste, wenn Sie die Nachrichten dieser Personen filtern möchten.

So entfernen Sie Freunde:

1. Klicken Sie im Menü "Erweitert" auf **Konfigurieren**.
2. Klicken Sie im Fenster "Konfigurieren" auf **E-Mail & IM**.
3. Klicken Sie unter **Spam-Schutz** auf **Erweitert**.
4. Klicken Sie im Fenster "Spam-Schutz" auf **Freunde**.
5. Wählen Sie den zu entfernenden Freund aus und klicken Sie dann auf **Entfernen.**

Automatisches Aktualisieren von Freunden

Um sicherzustellen, dass Sie alle Nachrichten von Ihren Freunden empfangen, können Sie deren Adressen aus Ihren Adressbüchern importieren oder automatische Aktualisierungen planen.

Manuelles Importieren von Adressbüchern

SpamKiller kann Ihre Adressbücher importieren und Ihre Freunde aktualisieren.

So importieren Sie Adressbücher manuell:

1. Klicken Sie im Menü "Erweitert" auf **Konfigurieren**.
2. Klicken Sie im Fenster "Konfigurieren" auf **E-Mail & IM**.
3. Klicken Sie unter **Spam-Schutz** auf **Erweitert**.
4. Klicken Sie im Fenster "Spam-Schutz" auf **Adressbücher**.
5. Wählen Sie das zu importierende Adressbuch aus und klicken Sie auf **Jetzt ausführen**.
6. Klicken Sie auf **OK**.

Hinzufügen von Adressbüchern

Fügen Sie das Adressbuch zum Importvorgang hinzu, damit gewährleistet ist, dass Sie alle Nachrichten von Ihren Freunden empfangen.

So fügen Sie Adressbücher hinzu:

1. Klicken Sie im Menü "Erweitert" auf **Konfigurieren**.
2. Klicken Sie im Fenster "Konfigurieren" auf **E-Mail & IM**.
3. Klicken Sie unter **Spam-Schutz** auf **Erweitert**.
4. Klicken Sie im Fenster "Spam-Schutz" auf **Adressbücher**.
5. Klicken Sie im Fenster "Adressbücher" auf **Hinzufügen**.
6. Wählen Sie den Typ des zu importierenden Adressbuchs in der Liste **Typ** aus.
7. Wählen Sie, sofern zutreffend, die Quelle des Adressbuchs in der Liste **Quelle** aus.
8. Klicken Sie in der Liste **Zeitplan** auf **Täglich**, **Wöchentlich** oder **Monatlich**, um festzulegen, wann SpamKiller Ihr Adressbuch auf neue Adressen prüfen soll.
9. Klicken Sie auf **OK**.

Bearbeiten von Adressbüchern

SpamKiller kann Ihre Adressbücher in regelmäßigen Intervallen importieren und die Informationen zu Ihren Freunde aktualisieren. Sie können auch Adressbücher bearbeiten und den Zeitplan für das Importieren ändern.

So bearbeiten Sie Adressbücher:

1. Klicken Sie im Menü "Erweitert" auf **Konfigurieren**.
2. Klicken Sie im Fenster "Konfigurieren" auf **E-Mail & IM**.
3. Klicken Sie unter **Spam-Schutz** auf **Erweitert**.
4. Klicken Sie im Fenster "Spam-Schutz" auf **Adressbücher**.
5. Wählen Sie das zu bearbeitende Adressbuch aus und klicken Sie anschließend auf **Bearbeiten**.
6. Führen Sie einen der folgenden Schritte aus:
   - Wählen Sie den Typ des zu importierenden Adressbuchs in der Liste **Typ** aus.
   - Wählen Sie, sofern zutreffend, die Quelle des Adressbuchs in der Liste **Quelle** aus.
   - Klicken Sie in der Liste **Zeitplan** auf **Täglich**, **Wöchentlich** oder **Monatlich**, um festzulegen, wann SpamKiller Ihr Adressbuch auf neue Adressen prüfen soll.
7. Klicken Sie auf **OK**.

Entfernen von Adressbüchern

Wenn aus einem bestimmten Adressbuch keine Adressen mehr automatisch importiert werden sollen, können Sie den entsprechenden Eintrag entfernen.

So entfernen Sie ein Adressbuch aus dem automatischen Importvorgang:

1. Klicken Sie im Menü "Erweitert" auf **Konfigurieren**.
2. Klicken Sie im Fenster "Konfigurieren" auf **E-Mail & IM**.
3. Klicken Sie unter **Spam-Schutz** auf **Erweitert**.
4. Klicken Sie im Fenster "Spam-Schutz" auf **Adressbücher**.
5. Wählen Sie das zu entfernende Adressbuch aus und klicken Sie anschließend auf **Entfernen**.

KAPITEL 28

Ändern von Filteroptionen

Filteroptionen ermöglichen das Ändern der Filterstufe, das Ändern spezieller Filter, das Anpassen der Handhabung von Nachrichten, das Angeben der zu filternden Zeichensätze und das Senden von Spam-Nachrichten an McAfee.

In diesem Kapitel

Ändern der Filterung von E-Mail-Nachrichten.....216
Ändern der Vorgehensweise,
wie Nachrichten verarbeitet werden 218
Filtern von Nachrichten mit Zeichensätzen 219
Melden von Spam-Nachrichten.....220

Ändern der Filterung von E-Mail-Nachrichten

Sie können festlegen, wie umfassend Ihre Nachrichten gefiltert werden sollen. Wenn legitime E-Mail-Nachrichten gefiltert werden, können Sie die Filterstufe herabsetzen.

Sie können bestimmte Filter auch aktivieren oder deaktivieren. Beispielsweise werden Nachrichten, die hauptsächlich Bilder enthalten, standardmäßig gefiltert. Wenn Sie diese Nachrichten empfangen möchten, können Sie diesen Filter deaktivieren.

Ändern der Filterstufe für E-Mail-Nachrichten

Sie können festlegen, wie umfassend Ihre Nachrichten gefiltert werden sollen. Wenn beispielsweise legitime E-Mail-Nachrichten gefiltert werden, können Sie die Filterstufe herabsetzen.

So ändern Sie die Filterstufe für E-Mail-Nachrichten:

1. Klicken Sie im Menü "Erweitert" auf **Konfigurieren**.
2. Klicken Sie im Fenster "Konfigurieren" auf **E-Mail & IM**.
3. Klicken Sie unter **Spam-Schutz** auf **Erweitert**.
4. Klicken Sie im Fenster "Spam-Schutz" auf **Filteroptionen**.
5. Verschieben Sie unter **Filteroptionen** den Schieberegler auf eine der folgenden Optionen:
   - **Niedrig**: Die meisten E-Mails werden akzeptiert.
   - **Mittel – Niedrig**: Es werden nur Nachrichten blockiert, die offensichtlich Spam-Nachrichten sind.
   - **Mittel**: Die meisten E-Mails werden akzeptiert.
   - **Mittel – Hoch**: Alle E-Mail-Nachrichten, die wie Spam aussehen, werden gefiltert.
   - **Hoch**: Nur Nachrichten von Absendern in der Freunde-Liste werden akzeptiert.
6. Klicken Sie auf **OK**.

Ändern spezieller Filter

Sie können bestimmte Filter aktivieren oder deaktivieren. Nachrichten, die hauptsächlich Bilder enthalten, werden beispielsweise immer gefiltert. Wenn Sie diese Nachrichten empfangen möchten, können Sie diesen Filter deaktivieren.

So ändern Sie spezielle Filter:

1. Klicken Sie im Menü "Erweitert" auf **Konfigurieren**.
2. Klicken Sie im Fenster "Konfigurieren" auf **E-Mail & IM**.
3. Klicken Sie unter **Spam-Schutz** auf **Erweitert**.
4. Wählen Sie **Filteroptionen**.
5. Aktivieren oder deaktivieren Sie unter **Spezielle Filter** folgende Kontrollkästchen:
   - **Filternachrichten mit verborgenem Text**: Verborgener Text wird verwendet, um eine Erkennung zu verhindern.
   - **Filternachrichten mit einem bestimmten Verhältnis von Bildern und Text**: Nachrichten, die hauptsächlich Bilder enthalten, sind in der Regel Spam.
   - **Filternachrichten mit absichtlichen HTML-Formatierungsfehlern**: Ungültige Formatierungen werden verwendet, um zu verhindern, dass Spam-Filter den Meldungstext korrekt interpretieren.
   - **Keine Nachrichten filtern, die größer sind als**: Nachrichten, die größer als die angegebene Größe sind, werden nicht gefiltert. Sie können die Nachrichtengröße erhöhen oder reduzieren (gültiger Bereich ist 0-250 KB).
6. Klicken Sie auf **OK**.

Ändern der Vorgehensweise, wie Nachrichten verarbeitet werden

Sie können ändern, wie Spam gekennzeichnet und verarbeitet wird. Sie können beispielsweise den Namen des Spam- oder Phish-Tags ändern und festlegen, ob die Nachricht in Ihrem Posteingang verbleiben oder in den SpamKiller-Ordner verschoben werden soll.

Ändern der Vorgehensweise, wie Nachrichten verarbeitet werden

Sie können ändern, wie Spam gekennzeichnet und verarbeitet wird. Sie können beispielsweise den Namen des Spam- oder Phish-Tags ändern und festlegen, ob die Nachricht in Ihrem Posteingang verbleiben oder in den SpamKiller-Ordner verschoben werden soll.

So legen Sie fest, wie Spam-Meldungen in SpamKiller verarbeitet werden:

1. Klicken Sie im Menü "Erweitert" auf **Konfigurieren**.
2. Klicken Sie im Fenster "Konfigurieren" auf **E-Mail & IM**.
3. Klicken Sie unter **Spam-Schutz** auf **Erweitert**.
4. Klicken Sie im Fenster "Spam-Schutz" auf **Verarbeitung**.
5. Führen Sie einen der folgenden Vorgänge aus:
   - Klicken Sie auf **Als Spam markieren und in den Ordner "Spamkiller" verschieben**.

     Dies ist die Standardeinstellung. Die Spam-Nachrichten werden in den Ordner "SpamKiller" verschoben.
   - Klicken Sie auf **Als Spam markieren und im Posteingang belassen**.

     Die Spam-Nachrichten verbleiben im Ihrem Posteingang.
   - Geben Sie im Feld **Dieses anpassbare Tag dem Betreff von Spam-Nachrichten hinzufügen** ein benutzerdefiniertes Tag ein.

     Das angegebene Tag wird der Betreffzeile von Spam-Nachrichten hinzugefügt.
   - Geben Sie im Feld **Dieses anpassbare Tag dem Betreff von Phishing-Nachrichten hinzufügen** ein benutzerdefiniertes Tag ein.

     Das angegebene Tag wird der Betreffzeile von Phishing-Nachrichten hinzugefügt.
6. Klicken Sie auf **OK**.

Filtern von Nachrichten mit Zeichensätzen

Zeichensätze werden zur Darstellung einer bestimmten Sprache verwendet, z. B. das für die Schrift verwendete Alphabet, die Ziffern und andere Symbole. Sie können E-Mails filtern, die bestimmte Zeichensätze enthalten. Sie sollten jedoch keine Zeichensätze für die Sprachen filtern, in denen Sie Ihre normalen E-Mails empfangen.

Wenn beispielsweise E-Mails in italienischer Sprache gefiltert werden sollen, dabei jedoch regelmäßig E-Mails in englischer Sprache eingehen, wählen Sie nicht die Option "Westeuropäisch". Mit der Option "Westeuropäisch" werden nicht nur italienische E-Mails blockiert, sondern auch Mails auf Englisch und in sämtlichen anderen Sprachen mit dem Zeichensatz "Westeuropäisch".

Nachrichten mit Zeichensätzen filtern

Sie können E-Mails filtern, die bestimmte Zeichensätze enthalten. Sie sollten jedoch keine Zeichensätze für die Sprachen filtern, in denen Sie Ihre normalen E-Mails empfangen.

So filtern Sie Nachrichten mit Zeichensätzen:

1. Klicken Sie im Menü "Erweitert" auf **Konfigurieren**.
2. Klicken Sie im Fenster "Konfigurieren" auf **E-Mail & IM**.
3. Klicken Sie unter **Spam-Schutz** auf **Erweitert**.
4. Klicken Sie im Fenster "Spam-Schutz" auf **Zeichensätze**.
5. Aktivieren Sie das Kontrollkästchen für die zu filternden Zeichensätze.
6. Klicken Sie auf **OK**.

Melden von Spam-Nachrichten

Sie können Spam-Nachrichten an McAfee senden, wo diese analysiert werden, um entsprechende Filter-Updates zu erstellen.

Spam-Nachrichten melden

Sie können Spam-Nachrichten an McAfee senden, wo diese analysiert werden, um entsprechende Filter-Updates zu erstellen.

So melden Sie Spam-Nachrichten an McAfee:

1. Klicken Sie im Menü "Erweitert" auf **Konfigurieren**.
2. Klicken Sie im Fenster "Konfigurieren" auf **E-Mail & IM**.
3. Klicken Sie unter **Spam-Schutz** auf **Erweitert**.
4. Klicken Sie im Fenster "Spam-Schutz" auf **Melden von Spam an McAfee**.
5. Aktivieren Sie eines der folgenden Kontrollkästchen:
   - **Berichte beim Klicken auf "Als Spam markieren" aktivieren**: Sendet jedes mal eine Nachricht an McAfee, wenn Sie diese als Spam markieren.
   - **Berichte beim Klicken auf "Nicht als Spam markieren" aktivieren**: Sendet jedes mal eine Nachricht an McAfee, wenn Sie diese nicht als Spam markieren.
   - **Gesamte Nachrichten senden (nicht nur Header)**: Sendet die gesamte Nachricht, einschließlich Header, wenn Sie eine Nachricht an McAfee sendet.
6. Klicken Sie auf **OK**.

KAPITEL 29

Verwalten persönlicher Filter

In Filtern sind die Elemente definiert, nach denen in einer E-Mail gesucht wird.

SpamKiller verwendet viele Filter; Sie können jedoch neue Filter erstellen oder bestehende Filter bearbeiten, um zu optimieren, welche Nachrichten als Spam identifiziert werden. Wenn ein Filterausdruck beispielsweise "hypothek" enthält, sucht SpamKiller nach Nachrichten mit dem Wort "hypothek".

Prüfen Sie beim Hinzufügen von Filtern die Formulierung genau, die gefiltert werden soll. Wenn die Formulierung wahrscheinlich auch in normalen E-Mails vorkommt, verwenden Sie sie nicht.

In diesem Kapitel

Grundlagen zum Verwalten persönlicher Filter 222
Verwenden regulärer Ausdrücke.....225

Grundlagen zum Verwalten persönlicher Filter

In diesem Abschnitt wird beschrieben, wie Sie persönliche Filter verwalten.

Hinzufügen von persönlichen Filtern

Das Erstellen von Filtern ist optional, und sie werden auf eingehende Nachrichten angewandt. Erstellen Sie daher keine Filter mit gebräuchlichen Wörtern, die auch in normalen E-Mails ohne Spam-Absicht auftreten können.

So fügen Sie einen Filter hinzu:

1. Klicken Sie im Menü "Erweitert" auf **Konfigurieren**.
2. Klicken Sie im Konfigurationsbereich auf **E-Mail & IM**.
3. Klicken Sie unter **Spam-Schutz** auf **Erweitert**.
4. Klicken Sie im Bereich "Spam-Schutz" auf **Persönliche Filter**.
5. Klicken Sie auf **Hinzufügen**.
6. Klicken Sie in der Liste **Element** auf einen Eintrag, um festzulegen, ob der Filter die Wörter oder Begriffe in der Betreffzeile, im Nachrichtentext, im Header oder im Absender der Nachricht sucht.
7. Klicken Sie in der Liste **Bedingung** auf einen Eintrag, um festzulegen, ob der Filter nach einer Nachricht sucht, die die festgelegten Wörter oder Begriffe enthält oder nicht enthält.
8. Geben Sie im Feld **Wörter oder Begriffe** ein, nach welchen Wörtern oder Begriffen in der Nachricht gesucht werden soll. Wenn Sie beispielsweise "hypothek" eingeben, werden alle Nachrichten, die dieses Wort enthalten, gefiltert.
9. Aktivieren Sie das Kontrollkästchen **Dieser Filter verwendet reguläre Ausdrücke (RegEx)**, um Zeichenmuster anzugeben, die in Filterbedingungen verwendet werden. Zum Testen eines Zeichenmusters klicken Sie auf **Testen**.
10. Klicken Sie auf **OK**.

Bearbeiten von persönlichen Filtern

In Filtern sind die Elemente definiert, nach denen in einer E-Mail gesucht wird. SpamKiller verwendet viele Filter; Sie können jedoch neue Filter erstellen oder bestehende Filter bearbeiten, um zu optimieren, welche Nachrichten als Spam identifiziert werden.

So bearbeiten Sie einen Filter:

1. Klicken Sie im Menü "Erweitert" auf **Konfigurieren**.
2. Klicken Sie im Konfigurationsbereich auf **E-Mail & IM**.
3. Klicken Sie unter **Spam-Schutz** auf **Erweitert**.
4. Klicken Sie im Bereich "Spam-Schutz" auf **Persönliche Filter**.
5. Wählen Sie den Filter aus, der bearbeitet werden soll, und klicken Sie dann auf **Bearbeiten**.
6. Klicken Sie in der Liste **Element** auf einen Eintrag, um festzulegen, ob der Filter die Wörter oder Begriffe in der Betreffzeile, im Nachrichtentext, im Header oder im Absender der Nachricht sucht.
7. Klicken Sie in der Liste **Bedingung** auf einen Eintrag, um festzulegen, ob der Filter nach einer Nachricht sucht, die die festgelegten Wörter oder Begriffe enthält oder nicht enthält.
8. Geben Sie im Feld **Wörter oder Begriffe** ein, nach welchen Wörtern oder Begriffen in der Nachricht gesucht werden soll. Wenn Sie beispielsweise "hypothek" eingeben, werden alle Nachrichten, die dieses Wort enthalten, gefiltert.
9. Aktivieren Sie das Kontrollkästchen **Dieser Filter verwendet reguläre Ausdrücke (RegEx)**, um Zeichenmuster anzugeben, die in Filterbedingungen verwendet werden. Zum Testen eines Zeichenmusters klicken Sie auf **Testen**.
10. Klicken Sie auf **OK**.

Entfernen persönlicher Filter

Nicht mehr benötigte Filter können entfernt werden. Die entfernten Filter werden dabei dauerhaft gelöscht.

So entfernen Sie einen Filter:

1. Klicken Sie im Menü "Erweitert" auf **Konfigurieren**.
2. Klicken Sie im Fenster "Konfigurieren" auf **E-Mail & IM**.
3. Klicken Sie unter **Spam-Schutz** auf **Erweitert**.
4. Klicken Sie im Fenster "Spam-Schutz" auf **Persönliche Filter**.
5. Wählen Sie den zu entfernenden Filter aus und klicken Sie dann auf **Entfernen**.
6. Klicken Sie auf **OK**.

Verwenden regulärer Ausdrücke

Reguläre Ausdrücke sind spezielle Zeichen und Sequenzen, die beim Definieren von Bedingungen verwendet werden können. Beispiel:

- Der regelmäßige Ausdruck **[0-9]*\.[0-9]+**

  Steht für Gleitkommazahlen mit nicht-ingenieurwissenschaftlicher Notation. Der reguläre Ausdruck findet: "12.12", ".1212" und "12.0", aber nicht "12" und "12".

- Der regelmäßige Ausdruck **\D*[0-9]+\D***

  Steht für alle Wörter mit Zahlen: "SpamKi11er" und "V1AGRA", aber nicht "SpamKiller" und "VIAGRA".

Regelmäßige Ausdrücke verwenden

Reguläre Ausdrücke sind spezielle Zeichen und Sequenzen, die beim Definieren von Bedingungen verwendet werden können.

****

Kennzeichnet, dass das nächste Zeichen entweder ein Sonderzeichen oder ein Buchstabe ist. Beispielsweise passt "n" zum Buchstaben "n". "\n" passt zu einem Zeichen für eine neue Zeile. Die Folge "\\" entspricht "\" und "\(" entspricht "(".

^

Steht für den Beginn der Eingabe.

$

Steht für das Ende der Eingabe.

*

Stimmt mit dem vorangehenden Zeichen kein oder mehrere Male überein. Beispielsweise passt "zo*" entweder auf "z" oder "zoo".

+

Stimmt mit dem vorangehenden Zeichen ein oder mehrere Male überein. Beispielsweise passt "zo+" bei "zoo", aber nicht bei "z".

?

Stimmt mit dem vorangehenden Zeichen kein oder ein Mal überein. Beispielsweise passt "a?ch?" auf die Zeichenfolge "ch" in "nicht".

.

Passt bei jedem einzelnen Zeichen außer einem Zeichen für eine neue Zeile.

(Muster)

Stimmt mit dem Muster überein und speichert die Übereinstimmung. Die übereinstimmende Unterzeichenfolge kann aus der verbleibenden Sammlung von Übereinstimmungen mit Hilfe von Element [0]...[n] ermittelt werden. Für eine Übereinstimmung mit den Klammerzeichen "(" und ")" verwenden Sie "\(" oder "\)".

x|y

Stimmt entweder mit "x" oder "y" überein. Zum Beispiel passt "z|boot" bei "z" oder "boot". "(z|b)oo" passt bei "zoo" oder "boot".

{n}

Das "n" steht für eine nicht negative Ganzzahl. Stimmt exakt n-Mal überein. Beispielsweise passt "u{2}" nicht bei einem "u" in "Ruth,", stimmt aber bei mit den ersten beiden "u" in "suuuuuuper" überein.

{n,}

Das "n" steht für eine nicht negative Ganzzahl. Stimmt mindestens n-Mal überein. Beispielsweise passt "u{2}" nicht bei einem "u" in "Ruth,", stimmt aber bei mit allen "u" in "suuuuuuper" überein. Der Ausdruck "u{1,}" entspricht "u+". Der Ausdruck "u{0,}" entspricht "u*".

{n,m}

Die Zeichen "m" und "n" stehen für nicht negative Ganzzahlen. Stimmt mindestens n-Mal und höchstens m-Mal überein. Beispielsweise passt "u{1,3}" auf die ersten drei Buchstaben "u" in "suuuuuuper". Der Ausdruck "u{0,1,}" entspricht "u?".

[xyz]

Ein Zeichensatz. Stimmt mit einem der enthaltenen Zeichen überein. Beispielsweise passt "[abc]" auf das "a" in "ganz".

[^xyz]

Ein negativer Zeichensatz. Passt auf jedes Zeichen, das nicht im Zeichensatz enthalten ist. Beispielsweise passt "[^abc]" auf das "g" in "ganz".

[a-z]

Ein Zeichenbereich. Passt auf jedes Zeichen innerhalb des angegebenen Bereichs. Beispielsweise würde “[a-z]“ auf jeden Klein- oder Großbuchstaben im Bereich von “a“ bis “z“ und “A“ bis “Z“ passen.

[A-Z]

Ein Zeichenbereich. Passt auf jedes Zeichen innerhalb des angegebenen Bereichs. Beispielsweise würde "[a-z]" auf jeden Groß- oder Kleinbuchstaben im Bereich von "A" bis "Z" und "a" bis "z" passen.

[^m-z]

Ein negativer Zeichenbereich. Passt auf jedes Zeichen, das sich nicht im angegebenen Bereich befindet. Beispielsweise würde "[^a-m]" auf jeden Kleinbuchstaben passen, der nicht zwischen "a" und "m" liegt.

\b

Entspricht einer Wortgrenze, d. h. der Position zwischen einem Wort und einem Leerzeichen. Beispielsweise würde "ht\b" auf das "ht" in "nicht" passen, aber nicht auf das "ht" in "Leuchter".

\B

Entspricht einer Nicht-Wortgrenze. Beispielsweise passt "fr*o\B" auf das "fro" in "immer froh".

\d

Steht für ein Ziffernzeichen. Entspricht [0-9].

\D

Steht für ein Nicht-Ziffernzeichen. Entspricht dem Ausdruck [^0-9].

\f

Entspricht einem Vorschubzeichen.

\n

Steht für ein Zeichen einer neuen Zeile.

\r

Entspricht einem Zeilenumbruchszeichen.

\s

Passt auf jedes "weiße" Leerzeichen, einschließlich Leerzeichen, Tabulator, Seitenvorschub usw. Entspricht "[\f\n\r\t\v]".

\S

Passt auf jedes "nicht weiße" Leerzeichen. Entspricht dem Ausdruck "[^ \f\n\r\t\v]".

\t

Steht für ein Tabulatorzeichen.

\v

Steht für ein vertikales Tabulatorzeichen.

\w

Passt auf jedes beliebige Wortzeichen einschließlich Unterstrich. Entspricht dem Ausdruck "[A-Za-z0-9_]".

\W

Passt auf jedes beliebige Nichtwortzeichen. Entspricht dem Ausdruck "[^A-Za-z0-9_]".

\num

Entspricht "num", wobei "num" eine positive Ganzzahl ist. Ein Rückverweis auf gespeicherte Übereinstimmungen. Beispielsweise stimmt "(.)\1" mit zwei aufeinander folgenden identischen Zeichen überein. "\n" steht für "n", wobei "n" ein oktaler Escape-Wert ist. Oktale Escape-Werte müssen eine Länge von 1, 2 oder 3 Ziffern besitzen. Zum Beispiel würden "\11" und "\011" beide mit einem Tabulatorzeichen übereinstimmen. "\0011" entspricht "\001" & "1". Oktale Escape-Werte dürfen nicht länger als 256 Zeichen sein; andernfalls würden nur die ersten beiden Ziffern den Ausdruck darstellen. Ermöglicht die Verwendung von ASCII-Code in regulären Ausdrücken.

\xn

Stimmt mit "n" überein, wobei "n" ein hexadezimaler Escape-Wert ist. Hexadezimale Escape-Werte müssen genau zwei Ziffern lang sein. Beispiel: “\x41“ stimmt mit “A“ überein. "\x041" entspricht "\x04" & "1". Ermöglicht die Verwendung von ASCII-Code in regulären Ausdrücken.

KAPITEL 30

Verwalten von SpamKiller

Das Verwalten von SpamKiller umfasst das Verwalten des Spam-Schutzes und der Verwendung der Symbolleisten.

Beim Verwalten des Spam-Schutzes können Sie das Filtern deaktivieren oder aktivieren.

Bei der Verwendung der Symbolleisten können Sie die E-Mail-Symbolleisten von SpamKiller aktivieren oder deaktivieren und Nachrichten über diese Symbolleiste als Spam markieren.

In diesem Kapitel

Verwalten des Spam-Schutzes 232
Verwenden von Symbolleisten.....233

Verwalten des Spam-Schutzes

Sie können das Filtern von E-Mail-Nachrichten aktivieren oder deaktivieren.

Deaktivieren Sie den Spam-Schutz, um zu verhindern, dass E-Mail-Nachrichten gefiltert werden. Aktivieren Sie den Spam-Schutz, um E-Mail-Nachrichten zu filtern.

Verwalten des Spam-Schutzes

Sie können den Spam-Schutz deaktivieren, so dass E-Mail-Nachrichten nicht gefiltert werden.

So deaktivieren Sie die Filterung:

1. Klicken Sie im Menü "Erweitert" auf **Konfigurieren**.
2. Klicken Sie im Fenster "Konfigurieren" auf **E-Mail & IM**.
3. Klicken Sie unter **Spam-Schutz** auf **Aus**.

Aktivieren des Spam-Schutzes

Sie können den Spam-Schutz aktivieren, so dass E-Mail-Nachrichten gefiltert werden.

So aktivieren Sie die Filterung:

1. Klicken Sie im Menü "Erweitert" auf **Konfigurieren**.
2. Klicken Sie im Fenster "Konfigurieren" auf **E-Mail & IM**.
3. Klicken Sie unter **Spam-Schutz** auf **Ein**.

Verwenden von Symbolleisten

Sie können E-Mail-Symbolleisten für unterstützte E-Mail-Clients aktivieren oder deaktivieren.

Wenn Sie eines der E-Mail-Programme Outlook, Outlook Express, Windows Mail, Eudora oder Thunderbird verwenden, können Sie außerdem Nachrichten von der SpamKiller-Symbolleiste aus als Spam oder Nicht-Spam markieren.

Deaktivieren einer Symbolleiste

Sie können Symbolleisten für unterstützte E-Mail-Clients deaktivieren.

So deaktivieren Sie eine Symbolleiste:

1. Klicken Sie im Menü "Erweitert" auf **Konfigurieren**.
2. Klicken Sie im Fenster "Konfigurieren" auf **E-Mail & IM**.
3. Klicken Sie unter **Spam-Schutz** auf **Erweitert**.
4. Klicken Sie im Fenster "Spam-Schutz" auf **E-Mail-Symbolleisten** und deaktivieren Sie das Kontrollkästchen neben der zu deaktivierenden Symbolleiste.
5. Klicken Sie auf **OK**.

Aktivieren einer Symbolleiste

Sie können deaktivierte Symbolleisten auch wieder aktivieren.

So aktivieren Sie eine Symbolleiste:

1. Klicken Sie im Menü "Erweitert" auf **Konfigurieren**.
2. Klicken Sie im Fenster "Konfigurieren" auf **E-Mail & IM**.
3. Klicken Sie unter **Spam-Schutz** auf **Erweitert**.
4. Klicken Sie im Fenster "Spam-Schutz" auf **E-Mail-Symbolleisten** und aktivieren Sie das Kontrollkästchen neben der zu aktivierenden Symbolleiste.
5. Klicken Sie auf **OK**.

Markieren von Nachrichten als Spam oder Nicht-Spam von der SpamKiller-Symbolleiste aus

Wenn Sie eines der E-Mail-Programme Outlook, Outlook Express, Windows Mail, Eudora oder Thunderbird verwenden, können Sie Nachrichten von der SpamKiller-Symbolleiste aus als Spam oder Nicht-Spam markieren.

Wenn Sie eine Nachricht als Spam markieren, wird die Nachricht mit dem Tag [SPAM] oder einem von Ihnen festgelegten Tag versehen und verbleibt in Ihrem Posteingang, Ihrem SpamKiller-Ordner (Outlook, Outlook Express, Windows Mail, Thunderbird) oder Ihrem Ordner für Junk-E-Mails (Eudora).

Wenn Sie eine Nachricht als Nicht-Spam markieren, wird der Nachrichten-Tag entfernt, und die Nachricht wird in Ihren Posteingang verschoben.

So markieren Sie Nachrichten von Outlook aus als Spam oder Nicht-Spam:

1. Wählen Sie in Ihrem E-Mail-Programm eine Nachricht aus.
2. Klicken Sie auf der Symbolleiste **SpamKiller** auf **Als Spam markieren** oder auf **Nicht als Spam markieren**.

So markieren Sie Nachrichten von Outlook Express, Windows Mail, Eudora oder Thunderbird aus als Spam oder Nicht-Spam:

1. Wählen Sie in Ihrem E-Mail-Programm eine Nachricht aus.
2. Klicken Sie im Menü **SpamKiller** auf **Als Spam markieren** oder auf **Nicht als Spam markieren**.

KAPITEL 31

Konfigurieren des Phishing-Schutzes

Unerwünschte E-Mail-Nachrichten werden als Spam (E-Mails, die Sie zum Kauf auffordern) oder als Phishing (E-Mails, mit denen Sie veranlasst werden, persönliche Daten auf einer Website preiszugeben, die in betrügerischer Absicht angelegt wurde) eingestuft.

Die Phishing-Filter helfen Ihnen, sich vor betrügerischen Websites zu schützen. Wenn Sie eine solche Website aufrufen, mit der betrügerische Absichten verbunden sind oder sein können, werden Sie zurück auf die Seite "McAfee Anti-Phishing-Filter" geleitet.

Sie können den Phishing-Schutz deaktivieren oder aktivieren oder die Filteroptionen ändern.

In diesem Kapitel

De-/Aktivieren des Phishing-Schutzes.....236
Ändern von Phishing-Filteroptionen.....237

De-/Aktivieren des Phishing-Schutzes

Sie können den Phishing-Schutz aktivieren oder deaktivieren. Deaktivieren Sie beispielsweise den Phishing-Schutz, wenn Sie versuchen, auf eine vertrauenswürdige Website zuzugreifen, diese aber blockiert ist.

Deaktivieren des Phishing-Schutzes

Deaktivieren Sie den Phishing-Schutz, wenn Sie versuchen, auf eine vertrauenswürdige Website zuzugreifen, diese aber blockiert ist.

So deaktivieren Sie den Phishing-Schutz:

1. Klicken Sie im Menü "Erweitert" auf **Konfigurieren**.
2. Klicken Sie im Fenster "Konfigurieren" auf **Internet & Netzwerk**.
3. Klicken Sie unter **Phishing** auf **Aus**.

Aktivieren des Phishing-Schutzes

Aktivieren Sie den Phishing-Schutz, um sicherzustellen, dass Sie vor Websites mit Phishing-Absichten geschützt sind.

So aktivieren Sie den Phishing-Schutz:

1. Klicken Sie im Menü "Erweitert" auf **Konfigurieren**.
2. Klicken Sie im Fenster "Konfigurieren" auf **Internet & Netzwerk**.
3. Klicken Sie unter **Phishing** auf **Ein**.

Ändern von Phishing-Filteroptionen

Es gibt zwei Möglichkeiten, wie McAfee ermittelt, ob eine Website eine Phishing-Site ist oder nicht: indem es die Website, die Sie aufrufen, mit einer Liste bekannter Sites mit Betrugsabsicht vergleicht, oder indem es versucht, festzustellen, ob die Website, die Sie anzeigen, betrügerische Absichten hat.

Phishing-Filteroptionen ändern

Es gibt zwei Möglichkeiten, wie McAfee ermittelt, ob eine Website eine Phishing-Site ist oder nicht: Lassen Sie beide Optionen aktiviert, um einen umfassenden Schutz zu gewährleisten.

So ändern Sie die Phishing-Schutz-Optionen:

1. Klicken Sie im Menü "Erweitert" auf **Konfigurieren**.
2. Klicken Sie im Fenster "Konfigurieren" auf **Internet & Netzwerk**.
3. Klicken Sie unter **Phishing** auf **Erweitert**.
4. Aktivieren oder deaktivieren Sie folgende Kontrollkästchen:
   - **Aktivieren Sie die Suche in Schwarzen und Weißen Listen, um betrügerische Websites zu entdecken**: Vergleicht die Website, die Sie anzeigen, mit einer Liste bekannter Sites mit betrügerischen Absichten.
   - **Heuristik aktivieren, um betrügerische Websites zu entdecken**: Versucht zu ermitteln, ob die Website, die Sie anzeigen, betrügerische Absichten hat.
5. Klicken Sie auf **OK**.

KAPITEL 32

Zusätzliche Hilfe

In diesem Kapitel werden häufig gestellte Fragen beschrieben.

In diesem Kapitel

Fragen und Antworten (FAQs) 240

Fragen und Antworten (FAQs)

In diesem Abschnitt finden Sie Antworten auf die häufigsten Fragen.

Was sind POP3-, MSN/Hotmail- und MAPI-Konten?

SpamKiller ist für die Verwendung mit diesen E-Mail-Kontotypen vorgesehen: POP3, POP3-Web-Mail, MSN/Hotmail und MAPI. Zwischen diesen Konten bestehen gewisse Unterschiede, die sich auf die Filterung in SpamKiller auswirken.

POP3

Dies ist der häufigste Kontotyp und gleichzeitig der Standardtyp für Internet-E-Mail. Bei einem POP3-Konto stellt SpamKiller eine direkte Verbindung zum Server her und filtert dort die E-Mails, bevor sie durch das E-Mail-Programm abgerufen werden.

POP3-Web-Mail

POP3-Web-Mail-Konten sind webbasiert.
POP3-Web-Mail-Konten werden auf ähnliche Weise wie POP3-Konten gefiltert.

MSN/Hotmail

MSN/Hotmail-Konten sind webbasiert. MSN/Hotmail-Konten werden auf ähnliche Weise gefiltert wie POP3-Konten.

MAPI

MAPI ist ein System von Microsoft, mit dem zahlreiche Messaging-Arten unterstützt werden, z. B. Internet-E- Mail, Fax oder Exchange Server-Messaging. MAPI wird daher häufig in Unternehmensumgebungen mit Microsoft®Exchange Server eingesetzt. Zahlreiche Benutzer verwenden allerdings Microsoft Outlook für persönliche Internet-E-Mails. SpamKiller kann auf MAPI-Konten zugreifen; hierbei ist jedoch Folgendes zu beachten:

- Die E-Mails werden in der Regel erst dann gefiltert, wenn sie durch das E-Mail-Programm abgerufen wurden.
- SpamKiller filtert ausschließlich den Standardposteingang und dort nur Internet-E-Mails.

Wozu dient der Phishing-Filter?

Unerwünschte E-Mail-Nachrichten werden als Spam (E-Mails, die Sie zum Kauf auffordern) oder als Phishing (E-Mails, mit denen Sie veranlasst werden, persönliche Daten auf einer Website preiszugeben, bei der es sich um Betrug handelt oder handeln könnte) eingestuft.

Der Phishing-Filter schützt Sie vor Websites, die auf einer schwarzen Liste (bestätigte Phishing-Websites oder zugehörige betrügerische Websites) oder auf einer grauen Liste (Seiten, die gefährliche Inhalte oder Links zu Websites auf der schwarzen Liste enthalten) stehen.

Wenn Sie eine solche Website aufrufen, mit der betrügerische Absichten verbunden sind oder sein können, werden Sie zurück auf die Seite "McAfee Anti-Phishing-Filter" geleitet.

Weshalb verwendet McAfee Cookies?

Die McAfee-Website verwendet Softwaretags, so genannte "Cookies", um Kunden bei einem erneuten Besuch der Website zu identifizieren. Cookies sind Textblöcke, die in einer Datei auf der Festplatte Ihres Computers abgelegt werden. Cookies dienen beim wiederholten Besuch einer Website zur Identifizierung.

McAfee nutzt Cookies zu folgenden Zwecken:

- Verwalten von Abonnementberechtigungen und Zulassungen
- Wiedererkennen des Benutzers beim nächsten Besuch auf der Website, so dass bei einem erneuten Besuch keine Registrierung erforderlich ist
- Ermitteln Ihres Konsumverhaltens und Abstimmen von Diensten auf Ihre Bedürfnisse
- Präsentieren von Informationen, Produkten und besonderen Angeboten, die für Sie von Interesse sein könnten

Sie werden von McAfee zur Angabe Ihres Vornamens gebeten, um den Umgang mit McAfee noch persönlicher zu gestalten.

Benutzer, deren Browser Cookies ablehnen, können die Abonnementdienste von McAfee nicht nutzen. Ihre Angaben werden weder an Dritte verkauft oder vermietet noch auf andere Weise zur Verfügung gestellt.

McAfee gestattet es Werbepartnern, in den Browsern der Besucher Cookies abzulegen. McAfee hat jedoch keinen Zugriff auf die Informationen, die in diesen Cookies gespeichert sind.

KAPITEL 33

McAfee Privacy Service

Privacy Service bietet umfassenden Schutz für Sie, Ihre Familie, Ihre persönlichen Daten und Ihren PC. Er hilft dabei, Sie vor Online-Identitätsdiebstahl zu schützen, die Übertragung persönlicher Informationen zu verhindern und potentiell anstößige Online-Inhalte (einschließlich Bilder, Anzeigen, Popups und Web-Bugs) zu filtern. Privacy Service bietet außerdem erweiterte Kindersicherungen, die es Erwachsenen ermöglichen, die Web-Browsing-Gewohnheiten ihrer Kinder zu überwachen, zu steuern und zu protokollieren. Es steht Ihnen darüber hinaus ein sicherer Speicherort für Kennwörter zur Verfügung.

Bevor Sie mit der Verwendung von Privacy Service beginnen, sollten Sie sich mit einigen der bekanntesten Funktionen vertraut machen. Details zur Konfiguration und Verwendung dieser Funktionen finden Sie in der Hilfe zu Privacy Service.

In diesem Kapitel

Funktionen 244
Einrichten der Kindersicherung.....245
Schützen von Informationen im Internet 267
Schützen von Kennwörtern.....273

Funktionen

Privacy Service bietet folgende Funktionen:

- Web-Browsing-Schutz
- Schutz persönlicher Daten
- Parental controls
- Kennwortspeicherung

Web-Browsing-Schutz

Mit dem Web-Browsing-Schutz können Sie Werbung, Popups und Web-Bugs auf Ihrem Computer blockieren. Durch das Blockieren von Werbung und Popups wird die Darstellung der meisten Werbeeinblendungen und Popup-Fenster in Ihrem Webbrowser verhindert. Durch das Blockieren von Web-Bugs wird verhindert, dass Websites Ihre Online-Aktivitäten nachverfolgen und persönliche Daten an nicht autorisierte Quellen übermitteln können. Zusammen verwendet erhöht das Blockieren von Werbung, Popups und Web-Bugs die Sicherheit und verhindert, dass das Surfen im Internet durch unerwünschte Inhalte gestört wird.

Schutz persönlicher Daten

Mit dem Schutz persönlicher Daten können Sie die Übertragung sensibler oder vertraulicher Informationen (z. B. Kreditkartennummern, Bankkontonummern, Adressen usw.) über das Internet blockieren.

Parental controls

Kindersicherungen ermöglichen das Konfigurieren von Inhaltsklassifikationen und Internetzugriffszeiten. Darin wird festgelegt, welche Inhalte und Websites ein Benutzer anzeigen kann und wann und wie lange dieser Benutzer auf das Internet zugreifen kann. Mit Kindersicherungen können Sie außerdem allgemeine Beschränkungen für den Zugriff auf bestimmte Websites festlegen oder den Zugriff auf der Grundlage von Altersgruppen und Stichwörtern gewähren oder blockieren.

Kennwortspeicherung

Der Kennwort-Tresor ist ein sicherer Speicherbereich für Ihre persönlichen Kennwörter. Er ermöglicht das sichere Speichern von Kennwörtern, so dass keine anderen Benutzer (auch kein McAfee- oder Systemadministrator) auf diese zugreifen können.

KAPITEL 34

Einrichten der Kindersicherung

Nachdem Sie einen Benutzer hinzugefügt haben, richten Sie die Kindersicherung für diesen Benutzer ein. Die Kindersicherung umfasst Einstellungen, die die Inhaltsklassifikationsgruppe, die Cookie-Blockierungsebene und zeitliche Internetbegrenzungen für diesen Benutzer festlegen. Die Inhaltsklassifikationsgruppe bestimmt auf der Grundlage der Altersgruppe eines Benutzers, auf welche Arten von Internetinhalten und Websites der Benutzer zugreifen kann. Die Cookie-Blockierungsebene bestimmt, ob Websites berechtigt sind, Cookies zu lesen, die sie auf dem Computer platzieren, wenn der Benutzer angemeldet ist. Die zeitlichen Internetbeschränkungen definieren die Tage und Zeiten, zu denen der Benutzer auf das Internet zugreifen kann.

Sie können auch globale Kindersicherungen einrichten, die für alle minderjährigen Benutzer gelten. Beispielsweise können Sie bestimmte Websites blockieren oder erlauben oder die Anzeige anstößiger Bilder verhindern, wenn minderjährige Benutzer im Internet surfen. Sie können auch globale Cookie-Blockierungseinstellungen für alle Benutzer festlegen. Wenn sich jedoch die Cookie-Blockierungsebene eines einzelnen Benutzers von den globalen Cookie-Blockierungseinstellungen unterscheidet, haben die globalen Einstellungen Priorität.

Hinweis: Sie müssen über Administratorrechte verfügen, um die Kindersicherung einzurichten.

In diesem Kapitel

Erstellen der Inhaltsklass.gruppe e. Benutzers 246
Festlegen der Cookie-Blockierungsebene eines Benutzers 248
Festlegen der Internet-Zugriffszeiten eines Benutzers 256
Blockieren von Websites.....257
Zulassen von Websites.....261
Zulassen, dass Websites Cookies platzieren 263
Blockieren potentiell anstößiger Web-Bilder.....265

Erstellen der Inhaltsklass.gruppe e. Benutzers

Ein Benutzer kann zu einer der folgenden Inhaltsklassifikationsgruppen gehören:

- Kleines Kind
- Kind
- Jüngerer Teenager
- Älterer Teenager
- Erwachsener

Inhalte werden auf der Grundlage der Altersgruppe, zu der der Benutzer gehört, bewertet (d. h. verfügbar gemacht oder blockiert). Beispielsweise werden bestimmte Websites für Benutzer blockiert, die zur Gruppe der kleinen Kinder gehören, jedoch für Benutzer der Gruppe der älteren Teenager verfügbar gemacht. Benutzer, die der Gruppe der Erwachsenen angehören, können auf alle Inhalte zugreifen. Standardmäßig wird ein neuer Benutzer automatisch der Gruppe "Kleines Kind" hinzugefügt, so dass der Inhalt, auf den er zugreifen kann, stark beschränkt ist.

Als Administrator können Sie die Inhaltsklassifikationsgruppe eines Benutzers festlegen und anschließend Websites auf der Grundlage dieser Gruppen blockieren oder erlauben. Wenn Sie Inhalte für einen Benutzer stärker begrenzen möchten, können Sie auch verhindern, dass der Benutzer Websites besucht, die nicht in der globalen Liste **Zulässige Websites** enthalten sind. Weitere Informationen finden Sie unter Blockieren von Websites auf der Grundlage von Stichwörtern (Seite 260) und Zulassen von Websites (Seite 261).

Erstellen der Inhaltsklass.gruppe e. Benutzers

Die Inhaltsklassifikationsgruppe eines Benutzers ist eine Altersgruppe, die die Arten von Internetinhalten bestimmt, die dem Benutzer zur Verfügung stehen.

So erstellen Sie die Inhaltsklassifikationsgruppe eines Benutzers:

1. Klicken Sie unter **Häufige Tasks** auf **Home**.
2. Klicken Sie unter **SecurityCenter-Informationen** auf **Konfigurieren**.
3. Klicken Sie im Bereich "SecurityCenter-Konfiguration" unter **Benutzer** auf die Option **Erweitert**.
4. Klicken Sie im Bereich "Benutzer" auf **Parental Controls**.
5. Wählen Sie in der Liste den Namen eines Benutzers aus.
6. Klicken Sie unter **Inhaltsklassifikation** auf die Altersgruppe, die Sie dem Benutzer zuweisen möchten.
   Sie können Inhalte anschließend entsprechend den

Altersgruppen bewerten, so dass Sie die Anzeige von Inhalten blockieren können, die für eine bestimmte Altersgruppe oder Entwicklungsstufe nicht angemessen sind.

7 Um zu verhindern, dass Benutzer Websites besuchen, die nicht in der globalen Liste **Zulässige Websites** enthalten sind, wählen Sie das Kontrollkästchen **Diesen Benutzer auf Websites einschränken in "Zulässige Websites"** aus.

8 Klicken Sie auf **OK**.

Festlegen der Cookie-Blockierungsebene eines Benutzers

Einige Websites erstellen kleine Dateien auf Ihrem Computer, sogenannte *Cookies*, um Ihre persönlichen Vorlieben und Surfgewohnheiten zu überwachen. Als Administrator können Sie einem Benutzer eine der folgenden Cookie-Blockierungsebenen zuweisen:

- Alle Cookies akzeptieren
- Alle Cookies ablehnen
- Cookies müssen vom Benutzer manuell akzeptiert werden

Die Einstellungen für das Akzeptieren aller Cookies erlaubt es Websites, die Cookies zu lesen, die sie auf Ihrem Computer platziert haben, als sich der entsprechende Benutzer angemeldet hat. Die Einstellung für das Ablehnen aller Cookies verhindert, dass Websites die Cookies lesen. Die Einstellung, dass der Benutzer aufgefordert werden soll, Cookies zu akzeptieren, fordert den Benutzer jedes Mal zum Akzeptieren eines Cookies auf, wenn eine Website versucht, ein Cookie auf Ihrem Computer zu platzieren. Der Benutzer kann von Fall zu Fall entscheiden, ob er die Cookies akzeptieren möchte. Nachdem der Benutzer entschieden hat, ob er Cookies für eine bestimmte Website akzeptieren oder ablehnen möchte, wird er für diese Website nicht wieder dazu aufgefordert.

Hinweis: Einige Websites erfordern, dass Cookies aktiviert sind, um einwandfrei funktionieren zu können.

Festlegen der Cookie-Blockierungsebene eines Benutzers

Einige Websites erstellen kleine Dateien auf Ihrem Computer, sogenannte *Cookies*, um Ihre persönlichen Vorlieben und Surfgewohnheiten zu überwachen. Sie können angeben, wie für jeden Benutzer Ihres Computers mit Cookies verfahren werden soll.

So legen Sie die Cookie-Blockierungsebene eines Benutzers fest:

1. Klicken Sie unter **Häufige Tasks** auf **Home**.
2. Klicken Sie unter **SecurityCenter-Informationen** auf **Konfigurieren**.
3. Klicken Sie im Bereich "SecurityCenter-Konfiguration" unter **Benutzer** auf die Option **Erweitert**.
4. Klicken Sie im Bereich "Benutzer" auf **Parental Controls**.
5. Wählen Sie in der Liste den Namen eines Benutzers aus.
6. Klicken Sie unter **Blockieren von Cookies** auf eine der folgenden Optionen:
   - **Alle Cookies akzeptieren:** Alle Websites, die dieser Bentzer anzeigt, können die an Ihren Computer gesendeten Cookies lesen.
   - **Alle Cookies ablehnen:** Keine der Websites, die dieser Bentzer anzeigt, können die an Ihren Computer gesendeten Cookies lesen.
   - **Cookies müssen vom Benutzer manuell akzeptiert werden:** Wenn dieser Benutzer versucht, eine Website anzuzeigen, wird eine Meldung angezeigt, in der der Benutzer dazu aufgefordert wird, Cookies zuzulassen oder abzulehnen.
7. Klicken Sie auf **OK**.

Hinzufügen einer Website zur Liste der akzeptierten Cookies eines Benutzers

Wenn Sie die Cookie-Blockierungsebene so festlegen, dass eine Genehmigung erteilt werden muss, damit Websites Cookies platzieren können, es aber bestimmten Websites stets erlauben möchten, Cookies ohne Genehmigung zu platzieren, können Sie diese Websites zur Liste der akzeptierten Cookies eines Benutzers hinzufügen.

So fügen Sie eine Website zur Liste der akzeptierten Cookies eines Benutzers hinzu:

1. Klicken Sie unter **Häufige Tasks** auf **Home**.
2. Klicken Sie unter **SecurityCenter-Informationen** auf **Konfigurieren**.
3. Klicken Sie im Bereich "SecurityCenter-Konfiguration" unter **Benutzer** auf die Option **Erweitert**.
4. Klicken Sie im Bereich "Benutzer" auf **Parental Controls**.
5. Wählen Sie in der Liste den Namen eines Benutzers aus.
6. Klicken Sie unter **Blockieren von Cookies** auf **Anzeigeliste**.
7. Geben Sie unter **Cookie-Websites akzeptieren** eine Website-Adresse in das Feld **http://** ein, und klicken Sie dann auf **Hinzufügen**.
8. Klicken Sie auf **Fertig**.

Ändern einer Website in der Liste der akzeptierten Cookies eines Benutzers

Wenn sich eine Website-Adresse ändert oder Sie sie beim Hinzufügen zur Liste der akzeptierten Cookies eine Benutzers falsch eingeben, können Sie sie anschließend bearbeiten.

So ändern Sie eine Website in der Liste der akzeptierten Cookies eines Benutzers:

1. Klicken Sie unter **Häufige Tasks** auf **Home**.
2. Klicken Sie unter **SecurityCenter-Informationen** auf **Konfigurieren**.
3. Klicken Sie im Bereich "SecurityCenter-Konfiguration" unter **Benutzer** auf die Option **Erweitert**.
4. Klicken Sie im Bereich "Benutzer" auf **Parental Controls**.
5. Wählen Sie in der Liste den Namen eines Benutzers aus.
6. Klicken Sie unter **Blockieren von Cookies** auf **Anzeigeliste**.
7. Klicken Sie unter **Cookie-Websites akzeptieren** auf einen Eintrag in der Liste **Websites**, ändern Sie die Website-Adresse im Feld **http://**, und klicken Sie dann auf **Aktualisieren**.
8. Klicken Sie auf **Fertig**.

Entfernen einer Website aus der Liste der akzeptierten Cookies eines Benutzers

Wenn Sie eine Website fälschlicherweise zur Liste der akzeptierten Cookies eines Benutzers hinzufügen, können Sie sie anschließend wieder entfernen.

So entfernen Sie eine Website aus der Liste der akzeptierten Cookies eines Benutzers:

1. Klicken Sie unter **Häufige Tasks** auf **Home**.
2. Klicken Sie unter **SecurityCenter-Informationen** auf **Konfigurieren**.
3. Klicken Sie im Bereich "SecurityCenter-Konfiguration" unter **Benutzer** auf die Option **Erweitert**.
4. Klicken Sie im Bereich "Benutzer" auf **Parental Controls**.
5. Wählen Sie in der Liste den Namen eines Benutzers aus.
6. Klicken Sie unter **Blockieren von Cookies** auf **Anzeigeliste**.
7. Klicken Sie unter **Cookie-Websites akzeptieren** auf einen Eintrag in der Liste **Websites**, und klicken Sie dann auf **Entfernen**.
8. Klicken Sie im Dialogfeld für die Bestätigung der Entfernung auf **Ja**.
9. Klicken Sie auf **Fertig**.

Hinzufügen einer Website zur Liste der abgelehnten Cookies eines Benutzers

Wenn Sie die Cookie-Blockierungsebene so festlegen, dass eine Genehmigung erteilt werden muss, damit Websites Cookies platzieren können, aber stets ohne Genehmigung verhindern möchten, dass bestimmte Websites Cookies platzieren, können Sie diese Websites zur Liste der abgelehnten Cookies eines Benutzers hinzufügen.

So fügen Sie eine Website zur Liste der abgelehnten Cookies eines Benutzers hinzu:

1. Klicken Sie unter **Häufige Tasks** auf **Home**.
2. Klicken Sie unter **SecurityCenter-Informationen** auf **Konfigurieren**.
3. Klicken Sie im Bereich "SecurityCenter-Konfiguration" unter **Benutzer** auf die Option **Erweitert**.
4. Klicken Sie im Bereich "Benutzer" auf **Parental Controls**.
5. Wählen Sie in der Liste den Namen eines Benutzers aus.
6. Klicken Sie unter **Blockieren von Cookies** auf **Anzeigeliste**.
7. Klicken Sie auf **Cookie-Websites ablehnen**.
8. Geben Sie unter **Cookie-Websites ablehnen** eine Website-Adresse in das Feld **http://** ein, und klicken Sie dann auf **Hinzufügen**.
9. Klicken Sie auf **Fertig**.

Ändern einer Website in der Liste der abgelehnten Cookies eines Benutzers

Wenn sich eine Website-Adresse ändert oder Sie sie beim Hinzufügen zur Liste der abgelehnten Cookies eines Benutzers falsch eingeben, können Sie sie anschließend bearbeiten.

So ändern Sie eine Website in der Liste der abgelehnten Cookies eines Benutzers:

1. Klicken Sie unter **Häufige Tasks** auf **Home**.
2. Klicken Sie unter **SecurityCenter-Informationen** auf **Konfigurieren**.
3. Klicken Sie im Bereich "SecurityCenter-Konfiguration" unter **Benutzer** auf die Option **Erweitert**.
4. Klicken Sie im Bereich "Benutzer" auf **Parental Controls**.
5. Wählen Sie in der Liste den Namen eines Benutzers aus.
6. Klicken Sie unter **Blockieren von Cookies** auf **Anzeigeliste**.
7. Klicken Sie auf **Cookie-Websites ablehnen**.
8. Klicken Sie unter **Cookie-Websites ablehnen** auf einen Eintrag in der Liste **Websites**, ändern Sie die Website-Adresse im Feld **http://**, und klicken Sie dann auf **Aktualisieren**.
9. Klicken Sie auf **Fertig**.

Entfernen einer Website aus der Liste der abgelehnten Cookies eines Benutzers

Wenn Sie fälschlicherweise eine Website zur Liste der abgelehnten Cookies eines Benutzers hinzufügen, können Sie sie anschließend wieder entfernen.

So entfernen Sie eine Website aus der Liste der abgelehnten Cookies eines Benutzers:

1. Klicken Sie unter **Häufige Tasks** auf **Home**.
2. Klicken Sie unter **SecurityCenter-Informationen** auf **Konfigurieren**.
3. Klicken Sie im Bereich "SecurityCenter-Konfiguration" unter **Benutzer** auf die Option **Erweitert**.
4. Klicken Sie im Bereich "Benutzer" auf **Parental Controls**.
5. Wählen Sie in der Liste den Namen eines Benutzers aus.
6. Klicken Sie unter **Blockieren von Cookies** auf **Anzeigeliste**.
7. Klicken Sie auf **Cookie-Websites ablehnen**.
8. Klicken Sie unter **Cookie-Websites ablehnen** auf einen Eintrag in der Liste **Websites**, und klicken Sie dann auf **Entfernen**.
9. Klicken Sie im Dialogfeld für die Bestätigung der Entfernung auf **Ja**.
10. Klicken Sie auf **Fertig**.

Festlegen der Internet-Zugriffszeiten eines Benutzers

Als Administrator können Sie das Internet-Zugriffszeitenraster verwenden, um festzulegen, wann und ob ein Benutzer auf das Internet zugreifen darf. Sie können einem Benutzer uneingeschränkten oder eingeschränkten Zugriff auf das Internet gewähren oder ihm den Zugriff ganz verbieten.

Im Zugriffszeitenraster können Sie Zugriffszeiten in 30-Minuten-Intervallen festlegen. Grüne Bereiche des Rasters stehen für Tage und Zeiträume, in denen ein Benutzer auf das Internet zugreifen kann. Rote Bereiche des Rasters stehen für Tage und Zeiträume, in denen einem Benutzer der Zugriff auf das Internet verweigert wird. Wenn ein Benutzer versucht, zu einer Zeit auf das Internet zuzugreifen, zu der dies für ihn nicht zulässig ist, wird er von McAfee benachrichtigt, dass der Internetzugriff zu diesem Zeitpunkt nicht möglich ist.

Wenn Sie einem Benutzer den Internetzugriff vollständig verwehren, kann sich dieser Benutzer anmelden und den Computer verwenden, jedoch nicht das Internet.

Festlegen der Internet-Zugriffszeiten eines Benutzers

Sie können das Internet-Zugriffszeitenraster verwenden, um festzulegen, wann ein bestimmter Benutzer auf das Internet zugreifen darf. Grüne Bereiche des Rasters stehen für Tage und Zeiträume, in denen ein Benutzer auf das Internet zugreifen kann. Rote Bereiche des Rasters stehen für Tage und Zeiträume, in denen einem Benutzer der Zugriff auf das Internet verweigert wird.

So legen Sie die Internet-Zugriffszeiten eines Benutzers fest:

1. Klicken Sie unter **Häufige Tasks** auf **Home**.
2. Klicken Sie unter **SecurityCenter-Informationen** auf **Konfigurieren**.
3. Klicken Sie im Bereich "SecurityCenter-Konfiguration" unter **Benutzer** auf die Option **Erweitert**.
4. Klicken Sie im Bereich "Benutzer" auf **Parental Controls**.
5. Wählen Sie in der Liste den Namen eines Benutzers aus.
6. Unter **Zugriffszeiten für das Internet** können Sie mittels "Ziehen-und-Ablegen" die Tage und Zeiten festlegen, zu denen dieser Benutzer auf das Internet zugreifen darf.
7. Klicken Sie auf **OK**.

Blockieren von Websites

Wenn Sie Administratorrechte haben und verhindern möchten, dass minderjährige Benutzer auf eine bestimmte Website zugreifen, können Sie die Website blockieren. Wenn ein Benutzer versucht, auf eine blockierte Website zuzugreifen, wird eine Nachricht angezeigt, die besagt, dass auf die Site nicht zugegriffen werden kann, weil sie von McAfee blockiert wurde.

Benutzer (einschließlich Administratoren), die der Altersstufe der Erwachsenen angehören, können auf alle Websites zugreifen, selbst wenn diese Websites in der Liste der **Blockierten Websites** enthalten sind. Zum Testen von blockierten Websites müssen Sie sich als nicht erwachsener Benutzer anmelden.

Als Administrator können Sie Websites auch auf der Grundlage der Stichwörter blockieren, die die Websites enthalten. McAfee unterhält eine Standardliste mit Stichwörtern und zugehörigen Regeln, die festlegen, ob ein Benutzer einer bestimmten Altersstufe auf eine Website zugreifen darf, die ein bestimmtes Stichwort enthält. Wenn Stichwort-Scans aktiviert sind, wird die Standardliste der Stichwörter verwendet, um Inhalte für Benutzer zu bewerten. Sie können jedoch Ihre eigenen zulässigen Stichwörter zur Standardliste hinzufügen und diese mit bestimmten Altersstufen verknüpfen. Von Ihnen hinzugefügte Stichwortregeln überschreiben Regeln, die möglicherweise mit einem identischen Stichwort in der Standardliste verknüpft sind. Sie können entweder bereits vorhandene oder neue Stichwörter mit bestimmten Altersstufen verknüpfen.

Blockieren einer Website

Sie können eine Website blockieren, wenn Sie verhindern möchten, dass minderjährige Benutzer auf diese Website zugreifen. Wenn ein Benutzer versucht, auf die Website zuzugreifen, wird eine Nachricht angezeigt, die besagt, dass die Site von McAfee blockiert wurde.

So blockieren Sie eine Website:

1. Klicken Sie unter **Häufige Tasks** auf **Home**.
2. Klicken Sie im Bereich "SecurityCenter Home" auf **Kindersicherungen**.
3. Klicken Sie im Abschnitt für die Informationen zur Kindersicherung auf **Konfigurieren**.
4. Vergewissern Sie sich im Bereich Konfiguration der Sicherung, dass Kindersicherungen aktiviert sind, und klicken Sie anschließend auf **Erweitert**.
5. Geben Sie im Bereich "Blockierte Websites" eine Website-Adresse in das Feld **http://** ein, und klicken Sie dann auf **Hinzufügen**.
6. Klicken Sie auf **OK**.

Ändern einer blockierten Website

Wenn sich eine Website-Adresse ändert oder Sie sie beim Hinzufügen zur Liste der blockierten Websites falsch eingeben, können Sie sie anschließend bearbeiten.

So ändern Sie eine blockierte Website:

1. Klicken Sie unter **Häufige Tasks** auf **Home**.
2. Klicken Sie im Bereich "SecurityCenter Home" auf **Kindersicherungen**.
3. Klicken Sie im Abschnitt für die Informationen zur Kindersicherung auf **Konfigurieren**.
4. Klicken Sie im Bereich "Konfiguration der Kindersicherung" auf die Option **Erweitert**.
5. Klicken Sie im Bereich "Blockierte Websites" auf einen Eintrag in der Liste **Blockierte Websites**, ändern Sie die Website-Adresse im Feld **http://**, und klicken Sie dann auf **Aktualisieren**.
6. Klicken Sie auf **OK**.

Entfernen einer blockierten Website

Wenn Sie eine Website nicht mehr blockieren möchten, müssen Sie sie aus der Liste **Blockierte Websites** entfernen.

So entfernen Sie eine blockierte Website:

1. Klicken Sie unter **Häufige Tasks** auf **Home**.
2. Klicken Sie im Bereich "SecurityCenter Home" auf **Kindersicherungen**.
3. Klicken Sie im Abschnitt für die Informationen zur Kindersicherung auf **Konfigurieren**.
4. Klicken Sie im Bereich "Konfiguration der Kindersicherung" auf die Option **Erweitert**.
5. Klicken Sie im Bereich "Blockierte Websites" auf einen Eintrag in der Liste **Blockierte Websites**, und klicken Sie dann auf **Entfernen**.
6. Klicken Sie im Dialogfeld für die Bestätigung der Entfernung auf **Ja**.
7. Klicken Sie auf **OK**.

Deaktivieren von Stichwort-Scans

Wenn Stichwort-Scans aktiviert sind, wird die McAfee-Standardliste der Stichwörter standardmäßig verwendet, um Inhalte für Benutzer zu bewerten. Auch wenn McAfee dies nicht empfiehlt, können Sie Stichwort-Scans jederzeit deaktivieren.

So deaktivieren Sie Stichwort-Scans:

1. Klicken Sie unter **Häufige Tasks** auf **Home**.
2. Klicken Sie im Bereich "SecurityCenter Home" auf **Kindersicherungen**.
3. Klicken Sie im Abschnitt für die Informationen zur Kindersicherung auf **Konfigurieren**.
4. Klicken Sie im Bereich "Konfiguration der Kindersicherung" auf die Option **Erweitert**.
5. Klicken Sie im Bereich "Globale Kindersicherungen" auf **Stichwort-Scans**.
6. Klicken Sie im Bereich "Stichwort-Scans" auf **Aus**.
7. Klicken Sie auf **OK**.

Blockieren von Websites auf der Grundlage von Stichwörtern

Wenn Sie Websites auf der Grundlage ihres Inhalts blockieren möchten, aber die genauen Website-Adressen nicht kennen, können Sie die Sites auf der Grundlage ihrer Stichwörter blockieren. Geben Sie einfach ein Stichwort ein und bestimmen Sie, welche Altersgruppen Websites, die dieses Stichwort enthalten, anzeigen können und welche dies nicht können.

So blockieren Sie Websites auf der Grundlage von Stichwörtern:

1. Klicken Sie unter **Häufige Tasks** auf **Home**.
2. Klicken Sie im Bereich "SecurityCenter Home" auf **Kindersicherungen**.
3. Klicken Sie im Abschnitt für die Informationen zur Kindersicherung auf **Konfigurieren**.
4. Klicken Sie im Bereich "Konfiguration der Kindersicherung" auf die Option **Erweitert**.
5. Klicken Sie im Bereich "Globale Kindersicherungen" auf **Stichwort-Scans**, und vergewissern Sie sich, dass diese Funktion aktiviert ist.
6. Klicken Sie im Bereich "Globale Kindersicherungen" auf **Stichwörter**.
7. Geben Sie in das Feld **Suchen nach** ein Stichwort ein. Websites, die dieses Wort enthalten, werden blockiert.
8. Bewegen Sie den Schieberegler **Mindestalter**, um eine Mindestaltergruppe anzugeben.
   Benutzer dieser und höherer Altersgruppen können Websites anzeigen, die das Stichwort enthalten.
9. Klicken Sie auf **OK**.

Zulassen von Websites

Wenn Sie über Administratorrechte verfügen, können Sie es allen Benutzern erlauben, auf eine bestimmte Website zuzugreifen, wodurch sämtliche Standardeinstellungen und blockierten Websites überschrieben werden.

Informationen zu blockierten Websites finden Sie unter Blockierte Websites (Seite 257).

Zulassen einer Website

Wenn Sie sicherstellen möchten, dass eine Website für keinen Benutzer blockiert wird, fügen Sie die Adresse der Website zur Liste **Zulässige Websites** hinzu. Wenn Sie eine Website zur Liste **Zulässige Websites** hinzufügen, überschreiben Sie sämtliche Standardeinstellungen und Websites, die zur Liste **Blockierte Websites** hinzugefügt wurden.

So lassen Sie eine Website zu:

1. Klicken Sie unter **Häufige Tasks** auf **Home**.
2. Klicken Sie im Bereich "SecurityCenter Home" auf **Kindersicherungen**.
3. Klicken Sie im Abschnitt für die Informationen zur Kindersicherung auf **Konfigurieren**.
4. Klicken Sie im Bereich "Konfiguration der Kindersicherung" auf die Option **Erweitert**.
5. Klicken Sie im Bereich "Globale Kindersicherungen" auf **Zulässige Websites**.
6. Geben Sie im Bereich "Zulässige Websites" eine Website-Adresse in das Feld **http://** ein, und klicken Sie dann auf **Hinzufügen**.
7. Klicken Sie auf **OK**.

Tipp: Sie können verhindern, dass ein Benutzer Websites besucht, die nicht in der Liste **Zulässige Websites** enthalten sind. Weitere Informationen finden Sie unter Erstellen der Inhaltsklassifikationsgruppe eines Benutzers (Seite 246).

Ändern einer zulässigen Website

Wenn sich eine Website-Adresse ändert oder Sie sie beim Hinzufügen zur Liste **Zulässige Websites** falsch eingeben, können Sie sie anschließend bearbeiten.

So ändern Sie eine zulässige Website:

1. Klicken Sie unter **Häufige Tasks** auf **Home**.
2. Klicken Sie im Bereich "SecurityCenter Home" auf **Kindersicherungen**.
3. Klicken Sie im Abschnitt für die Informationen zur Kindersicherung auf **Konfigurieren**.
4. Klicken Sie im Bereich "Konfiguration der Kindersicherung" auf die Option **Erweitert**.
5. Klicken Sie im Bereich "Globale Kindersicherungen" auf **Zulässige Websites**.
6. Klicken Sie im Bereich "Zulässige Websites" auf einen Eintrag in der Liste **Zulässige Websites**, ändern Sie die Website-Adresse im Feld **http://**, und klicken Sie dann auf **Aktualisieren**.
7. Klicken Sie auf **OK**.

Entfernen einer zulässigen Website

Sie können eine zulässige Website jederzeit entfernen. In Abhängigkeit von Ihren Einstellungen können McAfee-Benutzer möglicherweise nicht mehr auf eine Site zugreifen, wenn Sie diese aus der Liste **Zulässige Websites** entfernen.

So entfernen Sie eine zulässige Website:

1. Klicken Sie unter **Häufige Tasks** auf **Home**.
2. Klicken Sie im Bereich "SecurityCenter Home" auf **Kindersicherungen**.
3. Klicken Sie im Abschnitt für die Informationen zur Kindersicherung auf **Konfigurieren**.
4. Klicken Sie im Bereich "Konfiguration der Kindersicherung" auf die Option **Erweitert**.
5. Klicken Sie im Bereich "Globale Kindersicherungen" auf **Zulässige Websites**.
6. Klicken Sie im Bereich "Zulässige Websites" auf einen Eintrag in der Liste **Zulässige Websites**, und klicken Sie dann auf **Entfernen**.
7. Klicken Sie im Dialogfeld für die Bestätigung der Entfernung auf **Ja**.
8. Klicken Sie auf **OK**.

Zulassen, dass Websites Cookies platzieren

Wenn Sie für alle Websites verhindern, dass auf Ihrem Computer platzierte Cookies gelesen werden können, oder wenn Sie die Einstellungen für bestimmte Benutzer so konfigurieren, dass diese eine Nachricht erhalten, bevor Cookies akzeptiert werden, und dann merken, dass einige Websites nicht ordnungsgemäß funktionieren, können Sie es diesen Sites erlauben, ihre Cookies zu lesen.

Weitere Informationen zu Cookies und Cookie-Blockierungsebenen finden Sie unter Festlegen der Cookie-Blockierungsebene eines Benutzers (Seite 248).

Zulassen, dass eine Website Cookies platziert

Wenn Sie für alle Websites verhindern, dass auf Ihrem Computer platzierte Cookies gelesen werden können, oder wenn Sie die Einstellungen für bestimmte Benutzer so konfigurieren, dass diese eine Nachricht erhalten, bevor Cookies akzeptiert werden, und dann merken, dass einige Websites nicht ordnungsgemäß funktionieren, können Sie es diesen Sites erlauben, ihre Cookies zu lesen.

So lassen Sie zu, dass eine Website Cookies platziert:

1. Klicken Sie unter **Häufige Tasks** auf **Home**.
2. Klicken Sie im Bereich "SecurityCenter Home" auf **Kindersicherungen**.
3. Klicken Sie im Abschnitt für die Informationen zur Kindersicherung auf **Konfigurieren**.
4. Klicken Sie im Bereich "Konfiguration der Kindersicherung" auf die Option **Erweitert**.
5. Klicken Sie im Bereich "Globale Kindersicherungen" auf **Cookies**.
6. Geben Sie im Bereich "Cookies" eine Website-Adresse in das Feld **http://** ein, und klicken Sie dann auf **Hinzufügen**.
7. Klicken Sie auf **OK**.

Ändern der Liste "Akzeptierte Cookies"

Wenn sich eine Website-Adresse ändert oder Sie sie beim Hinzufügen zur Liste **Akzeptierte Cookies** falsch eingeben, können Sie sie anschließend bearbeiten.

So ändern Sie die Cookies-Liste:

1. Klicken Sie unter **Häufige Tasks** auf **Home**.
2. Klicken Sie im Bereich "SecurityCenter Home" auf **Kindersicherungen**.
3. Klicken Sie im Abschnitt für die Informationen zur Kindersicherung auf **Konfigurieren**.
4. Klicken Sie im Bereich "Konfiguration der Kindersicherung" auf die Option **Erweitert**.
5. Klicken Sie im Bereich "Globale Kindersicherungen" auf **Cookies**.
6. Klicken Sie im Bereich "Cookies" auf einen Eintrag in der Liste **Akzeptierte Cookies**, ändern Sie die Website-Adresse im Feld **http://**, und klicken Sie dann auf **Aktualisieren**.
7. Klicken Sie auf **OK**.

Verhindern, dass eine Website Cookies platziert

Wenn Sie verhindern möchten, dass eine bestimmte Website die Cookies liest, die sie auf Ihrem Computer platziert, können Sie die Website aus der Liste **Akzeptierte Cookies** entfernen.

So verhindern Sie, dass eine Website Cookies platziert:

1. Klicken Sie unter **Häufige Tasks** auf **Home**.
2. Klicken Sie im Bereich "SecurityCenter Home" auf **Kindersicherungen**.
3. Klicken Sie im Abschnitt für die Informationen zur Kindersicherung auf **Konfigurieren**.
4. Klicken Sie im Bereich "Konfiguration der Kindersicherung" auf die Option **Erweitert**.
5. Klicken Sie im Bereich "Globale Kindersicherungen" auf **Cookies**.
6. Klicken Sie im Bereich "Cookies" auf einen Eintrag in der Liste **Akzeptierte Cookies**, und klicken Sie dann auf **Entfernen**.
7. Klicken Sie im Dialogfeld für die Bestätigung der Entfernung auf **Ja**.
8. Klicken Sie auf **OK**.

Blockieren potentiell anstößiger Web-Bilder

Schützen Sie Ihre Familie, indem Sie die Anzeige potentiell anstößiger Bilder blockieren, wenn Sie im Internet surfen. Bilder können für alle Benutzer oder für alle Benutzer mit Ausnahme derjenigen blockiert werden, die der Altersgruppe der Erwachsenen angehören. Weitere Informationen zu Altersgruppen finden Sie unter Erstellen der Inhaltsklassifikationsgruppe eines Benutzers (Seite 246).

Standardmäßig ist die Bilderanalyse für alle Benutzer aktiviert, außer für die Mitglieder der Altersgruppe der Erwachsenen. Als Administrator können Sie diese Funktion jedoch jederzeit deaktivieren.

Blockieren potentiell anstößiger Bilder

Standardmäßig aktiviert McAfee die Bilderanalyse, die Ihre Familie schützt, indem sie während des Surfens im Internet die Anzeige potentiell anstößiger Bilder blockiert. Wenn McAfee ein potentiell anstößiges Bild erkennt, wird das Bild durch ein benutzerdefiniertes Bild ersetzt, das angibt, dass das Originalbild blockiert wurde. Wenn Sie die Bilderanalyse deaktivieren möchten, müssen Sie ein Administrator sein.

So blockieren Sie potentiell anstößige Bilder:

1. Klicken Sie unter **Häufige Tasks** auf **Home**.
2. Klicken Sie im Bereich "SecurityCenter Home" auf **Kindersicherungen**.
3. Klicken Sie im Abschnitt für die Informationen zur Kindersicherung auf **Konfigurieren**.
4. Klicken Sie im Bereich "Konfiguration der Kindersicherung" auf die Option **Erweitert**.
5. Klicken Sie im Bereich "Globale Kindersicherungen" auf **Bilderanalyse**.
6. Führen Sie im Bereich "Bilderanalyse" einen der folgenden Schritte aus:
   - Klicken Sie auf **Alle Benutzer**, um die Anzeige potentiell anstößiger Bilder für alle Benutzer zu blockieren.
   - Klicken Sie auf **Teenager und Kinder**, um die Anzeige potentiell anstößiger Bilder für alle Benutzer mit Ausnahme der Mitglieder der Altersgruppe der Erwachsenen zu blockieren.
7. Klicken Sie auf **OK**.

KAPITEL 35

Schützen von Informationen im Internet

Verwenden Sie Privacy Service, um Ihre Familie und Ihre persönlichen Informationen während des Surfens im Internet zu schützen. Wenn Sie beispielsweise Administrator sind, können Sie McAfee so konfigurieren, dass Anzeigen, Popups undWeb-Bugs blockiert werden, während sich der Benutzer im Internet bewegt. Sie können auch verhindern, dass Ihre persönlichen Informationen (wie Ihr Name, die Adresse, Kreditkartennummer und Kontonummern) über das Internet übertragen werden, indem Sie diese zum Bereich der blockierten Informationen hinzufügen.

In diesem Kapitel

Blockieren von Anzeigen, Popups und Web-Bugs....268
Blockieren von persönlichen Informationen.....270

Blockieren von Anzeigen, Popups und Web-Bugs

Wenn Sie Administrator sind, können Sie McAfee so konfigurieren, dass Anzeigen, Popups und Web-Bugs blockiert werden, während sich der Benutzer im Internet bewegt. Durch das Blockieren von Werbung und Popups wird die Darstellung der meisten Werbeeinblendungen und Popup-Fenster in Ihrem Webbrowser verhindert. Dies kann dazu beitragen, dass die Geschwindigkeit und Effizienz, mit der Sie sich im Internet bewegen, erhöht werden. Durch das Blockieren von Web-Bugs wird verhindert, dass Websites Ihre Online-Aktivitäten nachverfolgen und Informationen an nicht autorisierte Quellen übermitteln. Web-Bugs (auch Web-Beacons, Pixel-Tags, durchsichtige GIFs oder unsichtbare GIFs genannt) sind kleine Grafikdateien, die sich selbst in Ihre HTML-Seiten einbetten können und es einer nicht autorisierten Quelle erlauben, Cookies auf Ihrem Computer zu platzieren. Diese Cookies können dann Informationen an die nicht autorisierte Quelle übertragen.

Standardmäßig sind Anzeigen, Popups und Web-Bugs auf Ihrem Computer blockiert. Als Administrator können Sie Anzeigen, Popups oder Web-Bugs jederzeit zulassen.

Blockieren von Anzeigen

Sie können Anzeigen blockieren, während Benutzer im Internet surfen.

So blockieren Sie Werbung:

1. Klicken Sie unter **Häufige Tasks** auf **Home**.
2. Klicken Sie im Bereich "SecurityCenter Home" auf **Internet & Netzwerk**.
3. Klicken Sie im Abschnitt für die Informationen zu "Internet & Netzwerk" auf **Konfigurieren**.
4. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" unter **Web-Browsing-Schutz** auf die Option **Erweitert**.
5. Wählen Sie im Bereich "Werbungs-, Popup- & Web-Bug-Blockierung" das Kontrollkästchen **Anzeigen blockieren, die auf Webseiten angezeigt werden, während Sie im Internet surfen** aus.
6. Klicken Sie auf **OK**.

Blockieren von Popups

Sie können Popups blockieren, während Benutzer im Internet surfen.

So blockieren Sie Popups:

1. Klicken Sie unter **Häufige Tasks** auf **Home**.
2. Klicken Sie im Bereich "SecurityCenter Home" auf **Internet & Netzwerk**.
3. Klicken Sie im Abschnitt für die Informationen zu "Internet & Netzwerk" auf **Konfigurieren**.
4. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" unter **Web-Browsing-Schutz** auf die Option **Erweitert**.
5. Wählen Sie im Bereich "Werbungs-, Popup- & Web-Bug-Blockierung" das Kontrollkästchen **Popup-Fenster blockieren, die angezeigt werden, während Sie im Internet surfen** aus.
6. Klicken Sie auf **OK**.

Blockieren von Web-Bugs

Web-Bugs (auch Web-Beacons, Pixel-Tags, durchsichtige GIFs oder unsichtbare GIFs genannt) sind kleine Grafikdateien, die sich selbst in Ihre HTML-Seiten einbetten können und es einer nicht autorisierten Quelle erlauben, Cookies auf Ihrem Computer zu platzieren. Diese Cookies können dann Informationen an die nicht autorisierte Quelle übertragen. Sie können verhindern, dass Web-Bugs auf Ihren Computer geladen werden, indem Sie sie blockieren.

So blockieren Sie Web-Bugs:

1. Klicken Sie unter **Häufige Tasks** auf **Home**.
2. Klicken Sie im Bereich "SecurityCenter Home" auf **Internet & Netzwerk**.
3. Klicken Sie im Abschnitt für die Informationen zu "Internet & Netzwerk" auf **Konfigurieren**.
4. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" unter **Web-Browsing-Schutz** auf die Option **Erweitert**.
5. Wählen Sie im Bereich "Werbungs-, Popup- & Web-Bug-Blockierung" das Kontrollkästchen **Web-Bugs auf diesem Computer blockieren** aus.
6. Klicken Sie auf **OK**.

Blockieren von persönlichen Informationen

Verhindern Sie, dass Ihre persönlichen Informationen (wie Ihr Name, die Adresse, Kreditkartennummer und Kontonummern) über das Internet übertragen werden, indem Sie diese zum Bereich der blockierten Informationen hinzufügen. Wenn McAfee personenbezogene Informationen (Personal Identifiable Information) im ausgehenden Datenverkehr entdeckt, geschieht Folgendes:

- Wenn Sie ein Administrator sind, werden Sie gefragt, ob diese Informationen wirklich gesendet werden sollen.
- Wenn Sie kein Administrator sind, werden die blockierten Informationen durch Sternchen (*) ersetzt. Wenn Sie beispielsweise die E-Mail *Lance Armstrong gewinnt Rennen* senden und *Armstrong* als persönliche Information festgelegt ist, die blockiert werden soll, wird die E-Mail mit folgendem Wortlaut gesendet: *Lance ********* gewinnt Rennen*.

Sie können die folgenden Typen von persönlichen Informationen blockieren: Name, Adresse, Postleitzahl, Sozialversicherungsnummer, Telefonnummer, Kreditkartennummern, Kontonummern, Broker-Konten und Telefonkarten. Wenn Sie persönliche Informationen eines anderen Typs blockieren möchten, können Sie den Typ auf **andere** setzen.

Blockieren von persönlichen Informationen

Sie können die folgenden Typen von persönlichen Informationen blockieren: Name, Adresse, Postleitzahl, Sozialversicherungsnummer, Telefonnummer, Kreditkartennummern, Kontonummern, Broker-Konten und Telefonkarten. Wenn Sie persönliche Informationen eines anderen Typs blockieren möchten, können Sie den Typ auf **andere** setzen.

So blockieren Sie persönliche Informationen:

1. Klicken Sie unter **Häufige Tasks** auf **Home**.
2. Klicken Sie im Bereich "SecurityCenter Home" auf **Internet & Netzwerk**.
3. Klicken Sie im Abschnitt für die Informationen zu "Internet & Netzwerk" auf **Konfigurieren**.
4. Vergewissern Sie sich im Bereich "Internet & Netzwerkkonfiguration", dass der Schutz für persönliche Informationen aktiviert ist, und klicken Sie anschließend auf **Erweitert**.
5. Klicken Sie im Bereich "Blockierte Informationen" auf **Hinzufügen**.
6. Wählen Sie den Typ der zu blockierenden Informationen aus der Liste aus.
7. Geben Sie Ihre persönlichen Informationen ein, und klicken Sie auf **OK**.
8. Klicken Sie im Dialogfeld "Personal Information Protection" auf **OK**.

KAPITEL 36

Schützen von Kennwörtern

Der Kennwort-Tresor ist ein sicherer Speicherbereich für Ihre persönlichen Kennwörter. Er ermöglicht es Ihnen, Ihre Kennwörter sicher zu speichern in dem Wissen, dass kein anderer Benutzer (auch kein McAfee-Administrator oder Systemadministrator) darauf zugreifen kann.

In diesem Kapitel

Einrichten des Kennwort-Tresors 274

Einrichten des Kennwort-Tresors

Bevor Sie mit der Verwendung des Kennwort-Tresors beginnen, müssen Sie ein Kennwort für den Tresor festlegen. Nur Benutzer, denen dieses Kennwort bekannt ist, können auf Ihren Kennwort-Tresor zugreifen. Wenn Sie das Kennwort für Ihren Kennwort-Tresor vergessen, können Sie es zurücksetzen. Alle Kennwörter, die zuvor in Ihrem Kennwort-Tresor gespeichert waren, werden daraufhin gelöscht.

Nachdem Sie ein Kennwort für den Kennwort-Tresor festgelegt haben, können Sie Kennwörter zu Ihrem Tresor hinzufügen, sie bearbeiten oder daraus löschen.

Hinzufügen eines Kennworts zum Kennwort-Tresor

Wenn Sie Probleme haben, sich Ihre Kennwörter zu merken, können Sie diese zum Kennwort-Tresor hinzufügen. Der Kennwort-Tresor ist ein sicherer Speicherort, auf den nur Benutzer zugreifen können, denen das Kennwort für Ihren Kennwort-Tresor bekannt ist.

So fügen Sie ein Kennwort zum Kennwort-Tresor hinzu:

1. Klicken Sie unter **Häufige Tasks** auf **Home**.
2. Klicken Sie im Bereich "SecurityCenter Home" auf **Internet & Netzwerk**.
3. Klicken Sie im Abschnitt für die Informationen zu "Internet & Netzwerk" auf **Konfigurieren**.
4. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" unter **Personal Information Protection** auf die Option **Erweitert**.
5. Klicken Sie im Bereich "Personal Information Protection" auf **Kennwort-Tresor**.
6. Geben Sie Ihr Kennwort für den Kennwort-Tresor in das Feld **Kennwort** ein, und geben Sie es anschließend in das Feld **Kennwort bestätigen** ein.
7. Klicken Sie auf **Öffnen**.
8. Klicken Sie im Bereich "Kennwort-Tresor" auf **Hinzufügen**.
9. Geben Sie eine Beschreibung des Kennworts (z. B. wofür es gebraucht wird) in das Feld **Beschreibung** ein, und geben Sie das Kennwort anschließend in das Feld **Kennwort** ein.
10. Klicken Sie auf **Hinzufügen**, und klicken Sie anschließend auf **OK**.

Ändern eines Kennworts im Kennwort-Tresor

Um sicherzustellen, dass die Einträge in Ihrem Kennwort-Tresor stets genau und verlässlich sind, müssen Sie sie aktualisieren, wenn sich die Kennwörter ändern.

So ändern Sie ein Kennwort im Kennwort-Tresor:

1. Klicken Sie unter **Häufige Tasks** auf **Home**.
2. Klicken Sie im Bereich "SecurityCenter Home" auf **Internet & Netzwerk**.
3. Klicken Sie im Abschnitt für die Informationen zu "Internet & Netzwerk" auf **Konfigurieren**.
4. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" unter **Personal Information Protection** auf die Option **Erweitert**.
5. Klicken Sie im Bereich "Personal Information Protection" auf **Kennwort-Tresor**.
6. Geben Sie das Kennwort für Ihren Kennwort-Tresor in das Feld **Kennwort** ein.
7. Klicken Sie auf **Öffnen**.
8. Klicken Sie im Bereich "Kennwort-Tresor" auf einen Kennworteintrag, und klicken Sie anschließend auf **Bearbeiten**.
9. Geben Sie eine Beschreibung des Kennworts (z. B. wofür es gebraucht wird) in das Feld **Beschreibung** ein, oder ändern Sie das Kennwort anschließend im Feld **Kennwort**.
10. Klicken Sie auf **Hinzufügen**, und klicken Sie anschließend auf **OK**.

Entfernen eines Kennworts aus dem Kennwort-Tresor

Sie können ein Kennwort jederzeit aus dem Kennwort-Tresor entfernen. Sie können ein Kennwort, das Sie aus dem Tresor entfernt haben, nicht wiederbeschaffen.

So entfernen Sie ein Kennwort aus dem Kennwort-Tresor:

1. Klicken Sie unter **Häufige Tasks** auf **Home**.
2. Klicken Sie im Bereich "SecurityCenter Home" auf **Internet & Netzwerk**.
3. Klicken Sie im Abschnitt für die Informationen zu "Internet & Netzwerk" auf **Konfigurieren**.
4. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" unter **Personal Information Protection** auf die Option **Erweitert**.
5. Klicken Sie im Bereich "Personal Information Protection" auf **Kennwort-Tresor**.
6. Geben Sie das Kennwort für Ihren Kennwort-Tresor in das Feld **Kennwort** ein.
7. Klicken Sie auf **Öffnen**.
8. Klicken Sie im Bereich "Kennwort-Tresor" auf einen Kennworteintrag, und klicken Sie anschließend auf **Entfernen**.
9. Klicken Sie im Dialogfeld für die Bestätigung der Entfernung auf **Ja**.
10. Klicken Sie auf **OK**.

Zurücksetzen des Kennworts für den Kennwort-Tresor

Wenn Sie das Kennwort für Ihren Kennwort-Tresor vergessen, können Sie es zurücksetzen. Alle Kennwörter, die Sie zuvor in Ihren Kennwort-Tresor eingegeben haben, werden jedoch daraufhin gelöscht.

So setzen Sie das Kennwort für den Kennwort-Tresor zurück:

1. Klicken Sie unter **Häufige Tasks** auf **Home**.
2. Klicken Sie im Bereich "SecurityCenter Home" auf **Internet & Netzwerk**.
3. Klicken Sie im Bereich für die Informationen zu "Internet & Netzwerk" auf **Konfigurieren**.
4. Klicken Sie im Bereich "Internet & Netzwerkkonfiguration" unter **Personal Information Protection** auf die Option **Erweitert**.
5. Klicken Sie im Bereich "Personal Information Protection" auf **Kennwort-Tresor**.
6. Geben Sie unter **Kennwort-Tresor zurücksetzen** ein neues Kennwort in das Feld **Kennwort** ein, und geben Sie es anschließend in das Feld **Kennwort bestätigen** ein.
7. Klicken Sie auf **Zurücksetzen**.
8. Klicken Sie im Dialogfeld für die Bestätigung der Zurücksetzung des Kennworts auf **Ja**.

KAPITEL 37

McAfee Data Backup

Mit Data Backup können Sie Ihre Dateien auf CD oder DVD, auf einem USB-Laufwerk, einer externen Festplatte oder auf einem Netzlaufwerk archivieren und so einen Datenverlust vermeiden. Bei der lokalen Archivierung können Sie Ihre persönlichen Dateien auf CD oder DVD, auf einem USB-Laufwerk, einer externen Festplatte oder auf einem Netzlaufwerk archivieren (sichern). Damit erhalten Sie eine lokale Kopie Ihrer Datensätze, Dokumente und anderen für Sie wichtigen Unterlagen, auf die Sie im Fall eines Datenverlusts zurückgreifen können.

Bevor Sie mit der Verwendung von Data Backup beginnen, sollten Sie sich mit einigen der bekanntesten Funktionen vertraut machen. Details zur Konfiguration und Verwendung dieser Funktionen finden Sie in der Hilfe zu Data Backup. Stellen Sie außerdem sicher, dass genügend Archivierungsmedien vorhanden sind, um lokale Archive anlegen zu können.

In diesem Kapitel

Funktionen 280
Archivieren von Dateien 281
Arbeiten mit archivierten Dateien 291

Funktionen

Data Backup bietet die folgenden Funktionen zum Speichern und Wiederherstellen von Fotos, Musik und anderen wichtigen Dateien.

Lokal geplante Archivierung

Schützen Sie Ihre Daten durch die Archivierung von Dateien und Ordnern auf eine CD, eine DVD, ein USB-Laufwerk, eine externe Festplatte oder ein Netzlaufwerk. Wenn Sie die erste Archivierung initiiert haben, werden automatisch inkrementelle Archivierungen für Sie ausgeführt.

Wiederherstellung mit nur einem Klick

Wenn auf Ihrem Computer Dateien oder Ordner versehentlich gelöscht oder beschädigt werden, können Sie die zuletzt gesicherten Versionen von den verwendeten Archivierungsmedien wiederherstellen.

Komprimierung und Verschlüsselung

Ihre archivierten Dateien sind standardmäßig komprimiert, wodurch Speicherplatz auf den Archivierungsmedien eingespart wird. Als zusätzliche Sicherheitsmaßnahme werden Ihre Archive standardmäßig verschlüsselt.

KAPITEL 38

Archivieren von Dateien

Mit McAfee Data Backup können Sie die Dateien, die sich auf Ihrem Computer befinden, wahlweise auf CD oder DVD, auf einem USB-Laufwerk, einer externen Festplatte oder auf einem Netzlaufwerk archivieren. Durch diese Archivierung können Sie Ihre Daten bei Datenverlust oder Beschädigung schnell und einfach wiederherstellen.

Vor dem Archivieren legen Sie den standardmäßigen Archiv-Speicherort fest (CD, DVD, USB-Laufwerk, externe Festplatte, Netzlaufwerk). Einige Einstellungen sind bereits vordefiniert, beispielsweise die Ordner und die Dateitypen für die Archivierung; Sie können diese Einstellungen nach Bedarf ändern.

Sobald Sie die Optionen für das lokale Archiv eingerichtet haben, können Sie die Standardeinstellungen für die Ausführung von vollständigen Archivierungen oder Schnellarchivierungen bearbeiten. Darüber hinaus können Sie jederzeit eine manuelle Archivierung ausführen.

In diesem Kapitel

Festlegen von Archivoptionen 282
Ausführen von vollständigen Archivierungen und Schnellarchivierungen.....287

Festlegen von Archivoptionen

Vor dem Archivieren von Daten müssen einige Optionen für das lokale Archiv festgelegt werden, beispielsweise die überwachungs-Speicherorte und die überwachten Dateitypen. Die überwachungs-Speicherorte sind Ordner auf dem Computer, die Data Backup auf neue Dateien und Dateiänderungen überwacht. Die überwachten Dateitypen (beispielsweise .doc oder .xls) werden beim Archivieren der überwachungs-Speicherorte durch Data Backup erfasst. Standardmäßig überwacht Data Backup alle Dateitypen, die in den überwachungs-Speicherorten gespeichert sind.

Sie können zwei Arten von überwachungs-Speicherorten festlegen: Speicherorte mit umfassender überwachung und Speicherorte mit oberflächlicher überwachung. Bei einem Speicherort mit umfassender überwachung archiviert Data Backup die überwachten Dateitypen in diesem Ordner und in allen Unterordnern. Bei einem Speicherort mit oberflächlicher überwachung archiviert Data Backup lediglich die überwachten Dateitypen in diesem Ordner selbst (nicht die in den Unterordnern). Darüber hinaus können Sie Speicherorte angeben, die aus dem lokalen Archiv ausgeschlossen werden sollen. Standardmäßig sind der Windows-Desktop und der Ordner **Eigene Dokumente** als Speicherorte mit umfassender überwachung eingerichtet.

Sobald Sie die überwachten Dateitypen und die überwachungs-Speicherorte festgelegt haben, richten Sie den Archiv-Speicherort ein (also die CD, die DVD, das USB-Laufwerk, das externe Laufwerk oder das Netzlaufwerk, auf dem die archivierten Dateien gespeichert werden sollen.) Sie haben jederzeit die Möglichkeit, den Archiv-Speicherort zu ändern.

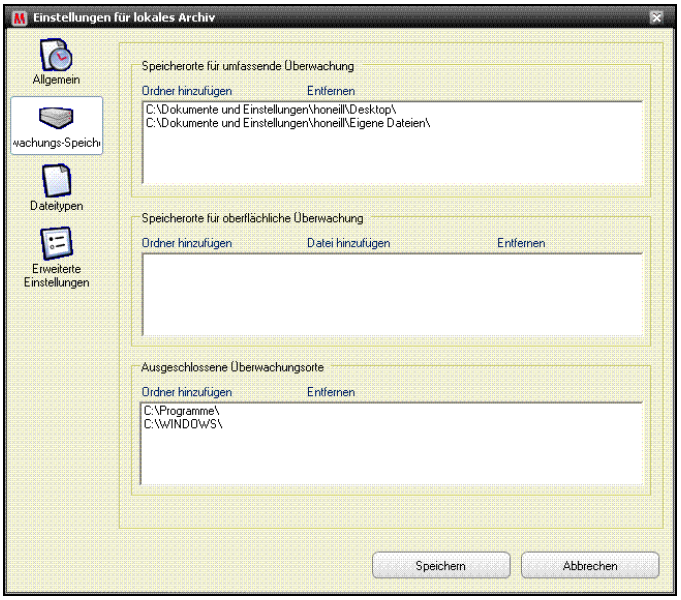
Aus Sicherheitsgründen bzw. zur Einschränkung des Umfangs sind die Verschlüsselung und die Komprimierung für die archivierten Dateien standardmäßig aktiviert. Bei der Verschlüsselung wird der Inhalt der Dateien in Code umgewandelt, so dass die Textinformationen für alle Benutzer unleserlich sind, denen das Verfahren zur Entschlüsselung unbekannt ist. Bei der Komprimierung werden die Dateien so "verdichtet", dass der erforderliche Speicherplatz zum Speichern oder übertragen auf ein Minimum reduziert wird. Auch wenn McAfee dies nicht empfiehlt, können Sie die Verschlüsselung und/oder die Komprimierung jederzeit deaktivieren.

Aufnehmen eines Speicherorts in das Archiv

Sie können zwei Arten von überwachungs-Speicherorten für die Archivierung festlegen: Speicherorte mit umfassender überwachung und Speicherorte mit oberflächlicher überwachung. Bei einem Speicherort mit umfassender überwachung überwacht Data Backup den Inhalt dieses Ordners und aller Unterordner auf änderungen. Bei einem Speicherort mit oberflächlicher überwachung überwacht Data Backup lediglich den Inhalt dieses Ordners (nicht den der Unterordner).

So nehmen Sie einen Speicherort in das Archiv auf:

1. Klicken Sie auf die Registerkarte **Lokales Archiv**.
2. Klicken Sie im linken Bereich auf **Einstellungen**.
3. Klicken Sie im Dialogfeld **Einstellungen für lokales Archiv** auf **überwachungs-Speicherorte**.



4. Führen Sie einen der folgenden Vorgänge aus:
   - Soll der Inhalt eines Ordners mit allen Unterordnern archiviert werden, klicken Sie unter **Speicherorte für umfassende überwachung** auf **Ordner hinzufügen**.
   - Soll nur der Inhalt eines Ordners archiviert werden (also nicht der Inhalt der Unterordner), klicken Sie unter **Speicherorte für oberflächliche überwachung** auf **Ordner hinzufügen**.

5 Wechseln Sie im Dialogfeld **Nach Ordner suchen** zum Ordner, der überwacht werden soll, und klicken Sie auf **OK**.

6 Klicken Sie auf **Speichern**.

Tipp: Soll Data Backup auch einen Ordner überwachen, den Sie noch nicht angelegt haben, dann können Sie im Dialogfeld **Nach Ordner suchen** mit der Option **Neuen Ordner erstellen** einen neuen Ordner erstellen und diesen Ordner gleichzeitig als neuen überwachungs-Speicherort festlegen.

Festlegen der Dateitypen für die Archivierung

Sie können die Dateitypen festlegen, die in den Speicherorten mit umfassender oder oberflächlicher überwachung archiviert werden sollen. Wählen Sie hierzu aus einer Liste mit Dateitypen, oder fügen Sie der Liste neue Dateitypen hinzu.

So legen Sie Dateitypen für die Archivierung fest:

1 Klicken Sie auf die Registerkarte **Lokales Archiv**.

2 Klicken Sie im linken Bereich auf **Einstellungen**.

3 Klicken Sie im Dialogfeld **Einstellungen für lokales Archiv** auf **Dateitypen**.

4 Erweitern Sie die Listen mit den Dateitypen, und aktivieren Sie das Kontrollkästchen neben den zu archivierenden Dateitypen.

5 Klicken Sie auf **Speichern**.

Tipp: Soll ein neuer Dateityp in die Liste **Ausgewählte Dateitypen** aufgenommen werden, geben Sie die Dateinamenerweiterung in das Feld **Benutzerdefinierten Dateityp zu "Andere" hinzufügen** ein, und klicken Sie auf **Hinzufügen**. Der neue Dateityp wird automatisch als überwachter Dateityp eingestuft.

Ausschließen eines Speicherorts aus dem Archiv

Wenn ein bestimmter Speicherort (Ordner) und dessen Inhalt nicht online archiviert werden sollen, schließen Sie diesen Speicherort aus der Archivierung aus.

So schließen Sie einen Speicherort aus der Archivierung aus:

1. Klicken Sie auf die Registerkarte **Lokales Archiv**.
2. Klicken Sie im linken Bereich auf **Einstellungen**.
3. Klicken Sie im Dialogfeld **Einstellungen für lokales Archiv** auf **überwachungs-Speicherorte**.
4. Klicken Sie auf **Ordner hinzufügen** unter **Ausgeschlossene überwachungs-Speicherorte**.
5. Wechseln Sie im Dialogfeld **Nach Ordner suchen** zum auszuschließenden Ordner. Markieren Sie diesen Ordner, und klicken Sie auf **OK**.
6. Klicken Sie auf **Speichern**.

Tipp: Soll Data Backup auch einen Ordner von der Sicherung ausschließen, den Sie noch nicht angelegt haben, dann können Sie im Dialogfeld **Nach Ordner suchen** mit der Option **Neuen Ordner erstellen** einen neuen Ordner erstellen und diesen Ordner gleichzeitig von der Sicherung ausschließen.

Ändern des Archiv-Speicherorts

Wenn Sie den Archiv-Speicherort ändern, werden die Dateien, die bislang an einem anderen Speicherort aktiviert wurden, als *Nie archiviert* aufgeführt.

So ändern Sie den Archiv-Speicherort:

1. Klicken Sie auf die Registerkarte **Lokales Archiv**.
2. Klicken Sie im linken Bereich auf **Einstellungen**.
3. Klicken Sie auf **Archiv-Speicherort ändern**.
4. Führen Sie im Dialogfeld **Archiv-Speicherort** einen der folgenden Schritte aus:
   - Klicken Sie auf **CD/DVD-Writer auswählen**, klicken Sie in der Liste **Writer** auf das CD- oder DVD-Laufwerk Ihres Computers, und klicken Sie auf **Speichern**.
   - Klicken Sie auf **Festplatten-Speicherort auswählen**, wechseln Sie zu einem USB-Laufwerk, einem lokalen Laufwerk oder einer externen Festplatte, markieren Sie das Speichermedium, und klicken Sie auf **OK**.

- Klicken Sie auf **Netzwerk-Speicherort auswählen**, wechseln Sie zu einem Netzlaufwerk, markieren Sie dieses Laufwerk, und klicken Sie auf **OK**.

5 überprüfen Sie, ob der neue Archiv-Speicherort unter **Archiv-Speicherort auswählen** richtig aufgeführt wird, und klicken Sie dann auf **OK**.

6 Klicken Sie im Bestätigungsdialogfeld auf **OK**.

7 Klicken Sie auf **Speichern**.

Deaktivieren der Verschlüsselung und Komprimierung für Archive

Durch das Verschlüsseln archivierter Dateien stellen Sie die Vertraulichkeit Ihrer Daten sicher. Der Inhalt der Dateien wird dabei unleserlich gemacht. Durch das Komprimieren werden archivierte Dateien auf die kleinstmögliche Größe "verdichtet". Standardmäßig sind die Verschlüsselung und die Komprimierung aktiviert; Sie können diese Optionen jedoch jederzeit deaktivieren.

So deaktivieren Sie die Verschlüsselung und die Komprimierung für Archive:

1 Klicken Sie auf die Registerkarte **Lokales Archiv**.

2 Klicken Sie im linken Bereich auf **Einstellungen**.

3 Klicken Sie im Dialogfeld **Einstellungen für lokales Archiv** auf **Erweiterte Einstellungen**.

4 Deaktivieren Sie das Kontrollkästchen **Verschlüsselung aktivieren, um die Sicherheit zu erhöhen**.

5 Deaktivieren Sie das Kontrollkästchen **Komprimierung aktivieren, um Speicherplatz zu reduzieren**.

6 Klicken Sie auf **Speichern**.

Hinweis: McAfee empfiehlt, die Verschlüsselung und die Komprimierung beim Archivieren der Dateien nicht zu deaktivieren.

Ausführen von vollständigen Archivierungen und Schnellarchivierungen

Es stehen zwei Arten von Archivierungen zur Auswahl: die vollständige Archivierung und die Schnellarchivierung. Bei einer vollständigen Archivierung werden alle Daten mit den angegebenen überwachten Dateitypen und an den definierten Speicherorten archiviert. Bei einer Schnellarchivierung werden nur die überwachten Dateien archiviert, die seit der letzten vollständigen Archivierung oder Schnellarchivierung geändert wurden.

Standardmäßig ist Data Backup so eingerichtet, dass montags um 9:00 Uhr eine vollständige Archivierung der überwachten Dateien an den überwachungs-Speicherorten ausgeführt wird, während jeweils 48 Stunden nach der letzten vollständigen Archivierung oder Schnellarchivierung eine Schnellarchivierung startet. Dieser Zeitplan sorgt dafür, dass stets ein aktuelles Archiv der Dateien vorliegt. Soll die Archivierung in anderen Zeitabständen erfolgen, können Sie den Zeitplan jederzeit nach Bedarf anpassen.

Zudem ist jederzeit eine manuelle Archivierung des Inhalts der überwachungs-Speicherorte möglich. Wenn Sie beispielsweise eine Datei geändert haben und die nächste vollständige Archivierung oder Schnellarchivierung mit Data Backup erst in einigen Stunden ansteht, können Sie die Dateien manuell archivieren. Bei einer manuellen Archivierung beginnt das Intervall für die automatischen Archivierungen wieder neu.

Darüber hinaus können Sie eine automatische oder manuelle Archivierung unterbrechen, wenn diese zu einem ungeeigneten Zeitpunkt ausgeführt wird. Wird beispielsweise eine automatische Archivierung gestartet, während Sie gerade eine ressourcenintensive Aufgabe ausführen, können Sie die Archivierung unterbrechen. Wenn Sie eine automatische Archivierung anhalten, beginnt das Intervall für die automatischen Archivierungen wieder neu.

Planen von automatischen Archivierungen

Sie können die Zeitabstände für vollständige Archivierungen und Schnellarchivierungen so einrichten, dass Ihre Daten stets geschützt sind.

So planen Sie automatische Archivierungen:

1. Klicken Sie auf die Registerkarte **Lokales Archiv**.
2. Klicken Sie im linken Bereich auf **Einstellungen**.
3. Klicken Sie im Dialogfeld **Einstellungen für lokales Archiv** auf **Allgemein**.
4. Soll täglich, wöchentlich oder monatlich eine vollständige Archivierung erfolgen, klicken Sie unter **Vollständige Archivierung alle** auf eine der folgenden Optionen:
   - **Tag**
   - **Woche**
   - **Monat**
5. Aktivieren Sie das Kontrollkästchen neben dem Tag, an dem die vollständige Archivierung ausgeführt werden soll.
6. Klicken Sie in der Liste **Um** einen Wert für die Uhrzeit an, zu der die vollständige Archivierung gestartet werden soll.
7. Soll täglich, wöchentlich oder monatlich eine Schnellarchivierung erfolgen, klicken Sie unter **Schnellarchivierung** auf eine der folgenden Optionen:
   - **Stunden**
   - **Tage**
8. Geben Sie in das Feld **Schnellarchivierung alle** den gewünschten Wert für die Häufigkeit ein.
9. Klicken Sie auf **Speichern**.

Unterbrechen einer automatischen Archivierung

Data Backup archiviert die Dateien an den überwachungs-Speicherorten automatisch gemäß dem definierten Zeitplan. Die Ausführung einer automatischen Archivierung kann jedoch jederzeit unterbrochen werden.

So unterbrechen Sie eine automatische Archivierung:

1. Klicken Sie im linken Bereich auf **Archivierung unterbrechen**.
2. Klicken Sie im Dialogfeld für die Bestätigung auf **Ja**.

Hinweis: Der Link **Archivierung unterbrechen** ist nur dann verfügbar, wenn gerade eine Archivierung ausgeführt wird.

Manuelles Ausführen einer Archivierung

Neben den automatischen Archivierungen, die nach einem bestimmten Zeitplan ablaufen, können Sie jederzeit eine manuelle Archivierung ausführen. Bei einer Schnellarchivierung werden nur die überwachten Dateien archiviert, die seit der letzten vollständigen Archivierung oder Schnellarchivierung geändert wurden. Bei einer vollständigen Archivierung werden die überwachten Dateitypen an allen überwachungs-Speicherorten erfasst.

So führen Sie eine manuelle vollständige Archivierung oder Schnellarchivierung aus:

1. Klicken Sie auf die Registerkarte **Lokales Archiv**.
2. Soll eine Schnellarchivierung ausgeführt werden, klicken Sie im linken Bereich auf **Schnellarchivierung**.
3. Soll eine vollständige Archivierung ausgeführt werden, klicken Sie im linken Bereich auf **Vollständige Archivierung**.
4. überprüfen Sie den Speicherplatz und die Einstellungen im Dialogfeld **Bereit, mit der Archivierung zu beginnen**, und klicken Sie auf **Fortfahren**.

KAPITEL 39

Arbeiten mit archivierten Dateien

Nach dem Archivieren können Sie mithilfe von Data Backup mit den archivierten Dateien arbeiten. Die archivierten Dateien werden in der gewohnten Explorer-Ansicht aufgeführt, so dass Sie die gewünschten Dateien schnell und einfach auffinden. Mit zunehmendem Umfang des Archivs können Sie die Dateien sortieren oder nach bestimmten Dateien suchen. Darüber hinaus lassen sich die Dateien direkt aus der Explorer-Ansicht heraus öffnen, so dass Sie deren Inhalt betrachten können, ohne die Dateien selbst abrufen zu müssen.

Wenn die lokale Kopie einer Datei veraltet ist, fehlt oder beschädigt wurde, können Sie diese Datei aus dem Archiv abrufen. Data Backup liefert außerdem die notwendigen Informationen zum Verwalten der lokalen Archive und der Speichermedien.

In diesem Kapitel

Verwenden des Explorers der lokale Archive 292
Wiederherstellen von archivierten Dateien 295
Verwalten von Archiven.....298

Verwenden des Explorers der lokale Archive

Im Explorer der lokalen Archive können Sie die lokal archivierten Dateien anzeigen und bearbeiten. Hier werden der Dateiname, der Typ, der Speicherort, die Größe, der Status (archiviert, nicht archiviert, Archivierung läuft) und das Datum der letzten Archivierung für die einzelnen Dateien aufgeführt. Darüber hinaus können Sie die Dateien nach diesen Kriterien sortieren.

Wenn Sie ein großes Archiv besitzen, können Sie schnell und einfach nach Dateien suchen. Geben Sie zunächst den Namen oder den Pfad der Datei (vollständig oder teilweise) ein, und verfeinern Sie dann die Suche, indem Sie die ungefähre Dateigröße und das Datum der letzten Archivierung angeben.

Eine gefundene Datei lässt sich direkt im Explorer der lokalen Archive öffnen. Data Backup öffnet die Datei im ursprünglichen Programm, so dass Sie änderungen an der Datei vornehmen können, ohne den Explorer der lokalen Archive verlassen zu müssen. Die Datei wird im bisherigen überwachungs-Speicherort auf dem Computer gespeichert und bei der automatischen Archivierung gemäß dem definierten Zeitplan berücksichtigt.

Sortieren von archivierten Dateien

Sie können die archivierten Dateien und Ordner nach den folgenden Kriterien sortieren: Dateiname, Dateityp, Größe, Status (archiviert, nicht archiviert, Archivierung läuft), Datum der letzten Archivierung, Speicherort (Pfad) auf dem Computer.

So sortieren Sie die archivierten Dateien:

1. Klicken Sie auf die Registerkarte **Lokales Archiv**.
2. Klicken Sie im rechten Bereich auf eine Spaltenüberschrift.

Suchen nach einer archivierten Datei

Wenn Sie ein großes Repository mit archivierten Dateien besitzen, können Sie schnell und einfach nach Dateien suchen. Geben Sie zunächst den Namen oder den Pfad der Datei (vollständig oder teilweise) ein, und verfeinern Sie dann die Suche, indem Sie die ungefähre Dateigröße und das Datum der letzten Archivierung angeben.

So suchen Sie nach einer archivierten Datei:

1. Geben Sie in das Feld **Suche** oben im Fenster den Dateinamen (vollständig oder teilweise) ein, und drücken Sie die EINGABETASTE.
2. Geben Sie in das Feld **Der gesamte oder ein Teil des Pfads** den Pfad (vollständig oder teilweise) ein.
3. Geben Sie die ungefähre Dateigröße der gesuchten Datei an. Führen Sie hierzu einen der folgenden Schritte aus:
   - Klicken Sie auf **< 100 KB**, **< 1 MB** oder **> 1 MB**.
   - Klicken Sie auf **Größe in KB**, und geben Sie die ungefähre Größe in das Feld ein.
4. Geben Sie das ungefähre Datum für die letzte Online-Sicherung der Datei an. Führen Sie hierzu einen der folgenden Schritte aus:
   - Klicken Sie auf **Diese Woche**, **Diesen Monat** oder **Dieses Jahr**.
   - Klicken Sie auf **Daten angeben**, klicken Sie in der Liste auf den Eintrag **Archiviert**, und wählen Sie dann in den Listen die ungefähren Werte für das Datum aus.
5. Klicken Sie auf **Suche**.

Hinweis: Falls Ihnen die ungefähre Größe und/oder das Datum der letzten Archivierung nicht bekannt sind, klicken Sie auf **Unbekannt**.

Öffnen einer archivierten Datei

Sie können eine archivierte Datei direkt im Explorer der lokalen Archive öffnen und so deren Inhalt betrachten.

So öffnen Sie archivierte Dateien:

1. Klicken Sie auf die Registerkarte **Lokales Archiv**.
2. Klicken Sie im rechten Bereich auf einen Dateinamen, und klicken Sie dann auf **öffnen**.

Tipp: Alternativ doppelklicken Sie auf den Dateinamen, um eine archivierte Datei zu öffnen.

Wiederherstellen von archivierten Dateien

Wenn eine Datei beschädigt ist, fehlt oder versehentlich gelöscht wurde, können Sie die jeweils letzte Kopie dieser Datei aus einem lokalen Archiv abrufen. Achten Sie daher darauf, Ihre Dateien in regelmäßigen Abständen zu archivieren. Darüber hinaus können Sie ältere Versionen von Dateien aus einem lokalen Archiv wiederherstellen. Wenn Sie beispielsweise eine Datei in regelmäßigen Abständen archivieren und nun zu einer früheren Version der Datei zurückkehren möchten, suchen Sie die Datei im Archiv-Speicherort. Liegt das Archiv auf einer lokalen Festplatte oder einem Netzlaufwerk vor, können Sie dieses Laufwerk direkt nach der Datei durchsuchen. Falls das Archiv sich auf einer externen Festplatte oder einem USB-Laufwerk befindet, schließen Sie das Laufwerk an den Computer an, und durchsuchen Sie dann das Laufwerk nach der Datei. Falls das Archiv auf einer CD oder DVD gespeichert ist, legen Sie die CD oder DVD in das entsprechende Laufwerk am Computer ein, und durchsuchen Sie dann den Datenträger nach der Datei.

Sie können auch Dateien wiederherstellen, die Sie von einem anderen Computer aus auf einem bestimmten Computer archiviert haben. Wenn Sie beispielsweise eine Reihe von Dateien auf Computer A auf eine externe Festplatte speichern, können Sie diese Dateien durchaus auf Computer B wiederherstellen. Installieren Sie hierzu McAfee Data Backup auf Computer B, und schließen Sie die externe Festplatte an diesen Computer an. Durchsuchen Sie den Datenträger dann in Data Backup nach den Dateien. Die Dateien werden in die Liste **Fehlende Dateien** für die Wiederherstellung eingetragen.

Weitere Informationen zum Archivieren von Dateien finden Sie unter Archivieren von Dateien. Falls Sie eine überwachte Datei aus dem Archiv löschen und dieses Löschen beabsichtigt war, können Sie auch den Eintrag in der Liste **Fehlende Dateien** entfernen.

Wiederherstellen von fehlenden Dateien aus einem lokalen Archiv

über das lokale Archiv von Data Backup können Sie Daten wiederherstellen, die in einem überwachungs-Ordner auf dem lokalen Computer fehlen. Wenn beispielsweise eine Datei, die bereits archiviert wurde, aus einem überwachungs-Ordner verschoben oder ganz gelöscht wird, können Sie die archivierte Datei aus dem lokalen Archiv wiederherstellen.

So rufen Sie eine fehlende Datei aus einem lokalen Archiv ab:

1. Klicken Sie auf die Registerkarte **Lokales Archiv**.
2. Aktivieren Sie unten im Fenster auf der Registerkarte **Fehlende Dateien** das Kontrollkästchen neben dem Namen der wiederherzustellenden Datei.
3. Klicken Sie auf **Wiederherstellen**.

Tipp: Sollen alle Dateien in der Liste **Fehlende Dateien** wiederhergestellt werden, klicken Sie auf **Alle wiederherstellen**.

Wiederherstellen einer älteren Version einer Datei aus einem lokalen Archiv

Soll eine ältere Version einer archivierten Datei wiederhergestellt werden, nehmen Sie diese Datei in die Liste **Fehlende Dateien** auf. Anschließend stellen Sie die Datei wie gewohnt aus der Liste **Fehlende Dateien** wieder her.

So stellen Sie eine ältere Version einer Datei aus einem lokalen Archiv wieder her:

1. Klicken Sie auf die Registerkarte **Lokales Archiv**.
2. Klicken Sie unten im Bildschirm auf der Registerkarte **Fehlende Dateien** auf **Durchsuchen**, und wechseln Sie dann zum Speicherort des Archivs.

   Für die Namen der Archivordner gilt das folgende Format: `cre ttmmjj_hh-mm-ss_***`, wobei gilt: `ttmmjj` ist das Datum, an dem die Dateien archiviert wurden, `hh-mm-ss` ist die Uhrzeit der Archivierung, und für `***` steht entweder `Full` oder `Inc`, je nachdem, ob eine vollständige Archivierung oder eine Schnellarchivierung durchgeführt wurde.
3. Wählen Sie den Speicherort aus, und klicken Sie anschließend auf **OK**.

   Die Dateien am ausgewählten Speicherort werden in die Liste **Fehlende Dateien** aufgenommen und können wiederhergestellt werden. Weitere Informationen finden Sie unter Wiederherstellen von fehlenden Dateien aus einem lokalen Archiv.

Entfernen von Dateien aus der Liste "Fehlende Dateien"

Wenn eine archivierte Datei aus einem überwachungs-Ordner verschoben oder ganz gelöscht wurde, wird diese Datei automatisch in die Liste **Fehlende Dateien** aufgenommen. Damit werden Sie darauf hingewiesen, dass eine Inkonsistenz zwischen den archivierten Dateien und den Dateien in den überwachungs-Ordnern vorliegt. Falls Sie die Datei aus dem überwachungs-Ordner verschieben oder ganz löschen und dieser Vorgang beabsichtigt war, können Sie die Datei aus der Liste **Fehlende Dateien** löschen.

So entfernen Sie eine Datei aus der Liste "Fehlende Dateien":

1. Klicken Sie auf die Registerkarte **Lokales Archiv**.
2. Aktivieren Sie unten im Fenster auf der Registerkarte **Fehlende Dateien** das Kontrollkästchen neben dem Namen der zu entfernenden Datei.
3. Klicken Sie auf **Löschen**.

Tipp: Sollen alle Dateien in der Liste **Fehlende Dateien** abgerufen werden, klicken Sie auf **Alle löschen**.

Verwalten von Archiven

Sie können jederzeit Informationen zu den vollständigen Archivierungen und den Schnellarchivierungen abrufen. Informieren Sie sich beispielsweise über den Umfang der derzeit überwachten Daten, die bereits archivierte Datenmenge und über den Umfang der Daten, die derzeit überwacht werden, jedoch noch nicht archiviert wurden. Darüber hinaus stehen Informationen zum Archivierungszeitplan bereit, beispielsweise das Datum der letzten Archivierung sowie der nächsten geplanten Archivierung.

Abrufen einer übersicht über die Archivierungsvorgänge

Sie können jederzeit Informationen zu Ihren Archivierungsvorgängen abrufen. Informieren Sie sich beispielsweise über den prozentualen Anteil der archivierten Dateien, über den Umfang der überwachten Daten, den Umfang der bereits archivierten Daten sowie über den Umfang der Daten, die überwacht werden, jedoch noch nicht archiviert wurden. Außerdem wird das Datum der letzten Archivierung und der nächsten geplanten Archivierung angezeigt.

So rufen Sie eine übersicht über die Archivierungsvorgänge ab:

1. Klicken Sie auf die Registerkarte **Lokales Archiv**.
2. Klicken Sie oben im Fenster auf **Kontozusammenfassung**.

KAPITEL 40

McAfee Wireless Network Security

Wireless Network Security bietet eine intuitive Benutzeroberfläche und aktuellen automatischen Schutz vor Datendiebstahl, unerlaubtem Netzwerkzugriff und Breitband-Downloads durch Eindringlinge. Das Programm verschlüsselt Ihre persönlichen Daten bei der Übertragung über Wi-Fi und verhindert, dass Hacker auf Ihr drahtloses Netzwerk zugreifen.

Wireless Network Security verhindert durch die folgenden Maßnahmen, dass Hacker Ihr drahtloses Netzwerk angreifen:

- Verhinderung nicht autorisierter Verbindungen zum Wi-Fi-Netzwerk,
- Verhinderung des Abfangens von Daten, die über ein Wi-Fi-Netzwerk übertragen werden,
- Erkennen von Verbindungsversuchen zu einem Wi-Fi-Netzwerk.

Wireless Network Security kombiniert benutzerfreundliche Funktionen, wie beispielsweise eine sofortige Netzwerksperre und das schnelle Hinzufügen legitimer Benutzer zum Netzwerk, mit robusten Sicherheitsfunktionen, wie beispielsweise automatische Schlüsselerstellung und planmäßige Schlüsselrotation.

In diesem Kapitel

Funktionen 300
Wireless Network Security starten 302
Drahtlose Netzwerke schützen 305
Drahtlosen Netzwerken verwalten 323
Sicherheit für drahtloses Netzwerk verwalten 337
Drahtlose Netzwerke überwachen.....353

Funktionen

Wireless Network Security bietet die folgenden Funktionen:

Ständig aktiver Schutz

Wireless Network Security erkennt und schützt automatisch gefährdete drahtlose Netzwerke, zu denen Sie eine Verbindung herstellen.

Leicht verständliche Benutzeroberfläche

Ermöglicht Ihnen den Schutz des Netzwerks, ohne dass Sie schwierige Entscheidungen treffen oder komplizierte technische Begriffe kennen müssen.

Starke automatische Verschlüsselung

Gewährt ausschließlich Familienangehörigen und Freunden Zugriff auf das Netzwerk und schützt Ihre Daten bei der Übertragung.

Reine Softwarelösung

Wireless Network Security funktioniert mit einem herkömmlichen drahtlosen Router oder Zugriffspunkt und mit normaler Sicherheitssoftware. Sie müssen keine zusätzliche Hardware erwerben.

Automatische Schlüsselrotation

Selbst die entschlossensten Hacker können Ihre Daten nicht abfangen, da der Schlüssel ständig geändert wird.

Hinzufügen von Netzwerkbenutzern

Sie können Ihren Familienangehörigen und Freunden mühelos Zugriff auf das Netzwerk gewähren. Sie können Benutzer drahtlos oder mittels Übertragungssoftware über ein USB-Laufwerk hinzufügen.

Intuitives Verbindungs-Tool

Das Tool für drahtlose Verbindungen ist intuitiv zu bedienen und informativ. Es zeigt Details zur Signalstärke und zum Sicherheitsstatus an.

Ereignisprotokollierung und Warnungen

Leicht verständliche Berichte und Warnungen bieten erfahrenen Benutzern weitere Informationen zum drahtlosen Netzwerk.

Aussetzmodus

Hiermit können Sie die Schlüsselrotation vorübergehend aussetzen, damit bestimmte Anwendungen ohne Unterbrechung ausgeführt werden können.

Kompatibilität mit anderer Hardware

Wireless Network Security aktualisiert sich selbst automatisch mit den neuesten Modulen für drahtlose Router oder Zugriffspunkte der am häufigsten verwendeten Marken. Dazu gehören: Linksys(R), NETGEAR(R), D-Link(R), Belkin(R), TRENDnet(R) und andere.

Wireless Network Security starten

Nach der Installation wird Wireless Network Security automatisch aktiviert. Ein manuelles Starten ist nicht notwendig. Optional können Sie drahtlosen Schutz auch manuell aktivieren und deaktivieren.

Nach der Installation von Wireless Network Security versucht Ihr Computer automatisch, eine Verbindung zum drahtlosen Router aufzubauen. Nachdem die Verbindung aufgebaut wurde, programmiert der Computer den Verschlüsselungsschlüssel in den drahtlosen Router. Wenn das Standardkennwort geändert wurde, erfolgt eine Kennwortabfrage, damit Wireless Network Security den drahtlosen Router mit dem gemeinsamen Verschlüsselungsschlüssel und einem hohen Sicherheitsmodus konfigurieren kann. Ihr Computer wird ebenfalls mit demselben freigegebenen Schlüssel und dem Verschlüsselungsmodus konfiguriert, wodurch eine sichere drahtlose Verbindung aufgebaut wird.

Wireless Network Security starten

Wireless Network Security ist standardmäßig aktiviert. Sie können drahtlosen Schutz allerdings auch manuell aktivieren und deaktivieren.

Die Aktivierung des drahtlosen Schutzes schützt Ihr drahtloses Netzwerk vor Intrusionen und Datenabfang. Besteht jedoch eine Verbindung mit einem externen drahtlosen Netzwerk, variiert Ihr Schutz in Abhängigkeit von der Sicherheitsebene.

So aktivieren Sie den drahtlosen Schutz manuell:

1. Führen Sie im Bereich "McAfee SecurityCenter" einen der folgenden Schritte aus:
   - Wählen Sie **Internet & Netzwerk**, und klicken Sie dann auf **Konfigurieren**.
   - Wählen Sie das Menü **Erweitert**, und dann im Bereich **Startseite** die Option **Konfigurieren**. Zeigen Sie auf **Internet & Netzwerk**.
2. Klicken Sie im Bereich **Internet & Netzwerkkonfiguration** unter **Drahtloser Schutz** auf **Ein**.

Hinweis: Wenn ein kompatibler drahtloser Adapter installiert ist, wird Wireless Network Security automatisch aktiviert.

Wireless Network Security deaktivieren

Wireless Network Security ist standardmäßig aktiviert. Sie können drahtlosen Schutz allerdings auch manuell aktivieren und deaktivieren.

Durch die Deaktivierung des drahtlosen Schutzes ist Ihr Netzwerk Intrusionen und Datenabfang schutzlos ausgeliefert.

So deaktivieren Sie den drahtlosen Schutz:

1. Führen Sie im Bereich "McAfee SecurityCenter" einen der folgenden Schritte aus:
   - Wählen Sie **Internet & Netzwerk**, und klicken Sie dann auf **Konfigurieren**.
   - Wählen Sie das Menü **Erweitert** und dann im Bereich **Startseite** die Option **Konfigurieren**. Zeigen Sie auf **Internet & Netzwerk**.
2. Klicken Sie im Bereich **Internet & Netzwerkkonfiguration** unter **Drahtloser Schutz** auf **Aus**.

KAPITEL 41

Drahtlose Netzwerke schützen

Wireless Network Security schützt Ihr Netzwerk durch die Einbindung drahtloser Verschlüsselung (entweder durch WEP, WPA oder WPA2, je nachdem, welche Ausstattung Sie haben). Es programmiert die Clients und drahtlosen Router automatisch mit den gültigen Verschlüsselungsschlüsseldaten, sodass der drahtlose Router Verbindungsautorisierungen für Computer erteilen kann. Drahtlose Netzwerke, die durch Verschlüsselung geschützt sind, sperren den Zugriff nicht autorisierter Benutzer auf das drahtlose Netzwerk. Weiterhin werden die Daten, die über ein drahtloses Netzwerk übertragen werden, geschützt. Wireless Network Security erreicht dies durch die folgenden Maßnahmen:

- Erstellung und Verteilung eines langen, starken, zufälligen und gemeinsamen Verschlüsselungsschlüssels,
- Planmäßiges Rotieren des Verschlüsselungsschlüssels,
- Konfiguration aller drahtlosen Geräte mit Verschlüsselungsschlüsseln.

In diesem Kapitel

Geschützte drahtlose Netzwerke einrichten 306
Computer zum geschützten drahtlosen Netzwerk hinzufügen 319

Geschützte drahtlose Netzwerke einrichten

Wenn Wireless Network Security installiert ist, erfolgt eine automatische Aufforderung zur Sicherung des unsicheren drahtlosen Netzwerks, mit dem Sie verbunden sind, oder zur Anmeldung an einem zuvor geschützten drahtlosen Netzwerk.

Wenn Sie nicht mit einem drahtlosen Netzwerk verbunden sind, sucht Wireless Network Security nach einem durch McAfee geschützten Netzwerk mit hoher Signalstärke und fordert den Benutzer auf, sich an diesem Netzwerk anzumelden. Sollten keine geschützten Netzwerke zur Verfügung stehen, sucht Wireless Network Security nach unsicheren Netzwerken mit starken Signalen. Wenn eines gefunden wurde, werden Sie aufgefordert, dieses Netzwerk zu schützen.

Alle drahtlosen Netzwerke, die nicht durch McAfee Wireless Network Security geschützt sind, werden von McAfee als "nicht geschützt" angesehen, auch wenn diese drahtlose Sicherheitsmechanismen, wie beispielsweise WEP und WPA, verwenden.

Alle drahtlosen Netzwerke, die nicht durch Wireless Network Security geschützt sind, werden von McAfee als nicht geschützt angesehen, auch wenn diese drahtlose Sicherheitsmechanismen, wie beispielsweise WEP und WPA, verwenden.

Über Zugriffstypen

Jeder drahtlose Computer, auf dem Wireless Network Security installiert ist, kann ein geschütztes drahtloses Netzwerk erstellen. Der erste Computer, der einen Router schützt und ein geschütztes drahtloses Netzwerk erstellt, erhält automatisch administrativen Zugriff auf dieses Netzwerk. Ein bestehender Benutzer mit administrativen Zugriffsrechten kann Computern, die sich später anmelden, administrative, vollständige oder Gast-Zugriffsrechte erteilen.

Computer mit administrativen oder vollständigen Zugriffstypen können die folgenden Aufgaben durchführen:

- Schutz und Entfernen eines Routers oder Zugriffspunkts,
- Rotieren von Sicherheitsschlüsseln,
- Ändern von Netzwerk-Sicherheitseinstellungen,
- Netzwerkreparaturen,
- Erteilung für Zugriffsberechtigungen für Computer auf das Netzwerk,
- Aufhebung von Zugriffsberechtigungen zum geschützten drahtlosen Netzwerk,
- Änderung der Administratorstufe eines Computers.

Computer mit Gast-Zugriffstypen können die folgenden Aufgaben durchführen:

- Herstellen einer Verbindung zu einem Netzwerk,
- Anmeldung an einem Netzwerk,
- Änderung von Einstellungen, die spezifisch für den Gastcomputer sind.

Hinweis: Computer können an einem drahtlosen Netzwerk über administrative Zugriffsrechte und an einem anderen über Gast- oder vollständige Zugriffsrechte verfügen. Ein Computer, der über Gast- oder vollständige Zugriffsrechte auf ein Netzwerk verfügt, kann ein neues Netzwerk erstellen.

Verwandte Themen

- Anmelden an einem geschützten drahtlosen Netzwerk (Seite 310)
- Computern administrativen Zugriff gewähren (Seite 316)
- Netzwerkzugriffsrechte aufheben (Seite 335)

Geschützte drahtlose Netzwerke erstellen

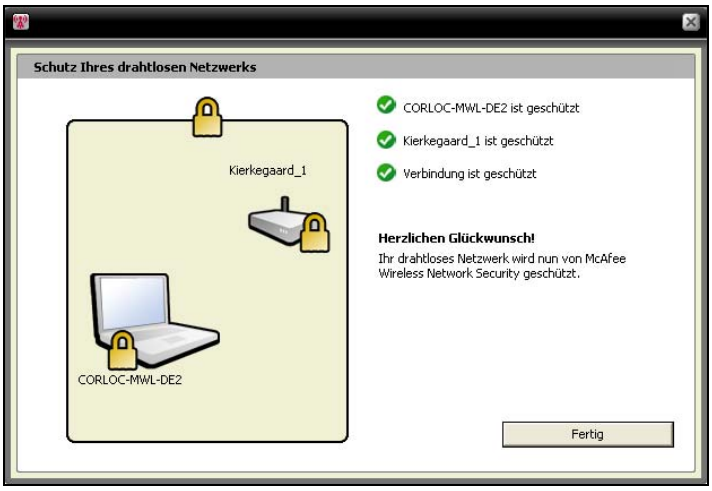
Um ein geschütztes drahtloses Netzwerk zu erstellen, müssen Sie zunächst den drahtlosen Router oder Zugriffspunkt des drahtlosen Netzwerks hinzufügen.

So fügen Sie einen drahtlosen Router oder Zugriffspunkt hinzu:

1. Klicken Sie mit der rechten Maustaste auf das Symbol für Wireless Network Security im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Tools anzeigen** aus.
3. Klicken Sie im Bereich "Sicherheitstools" unter **Drahtlosen Router/Zugriffspunkt schützen** auf **Schützen**.
4. Wählen Sie im Bereich "Drahtlosen Router/Zugriffspunkt schützen" ein drahtloses Netzwerk aus, das geschützt werden soll und klicken Sie auf **Schützen**.

Das Fenster "Schutz Ihres drahtlosen Netzwerks" wird geöffnet, während Wireless Network Security versucht, Ihren Computer, Router und die Netzwerkverbindung zu schützen.

Ein erfolgreicher Schutz all dieser Komponenten hat den gesamten Schutz Ihres drahtlosen Netzwerks zur Folge.



5 Klicken Sie auf **Fertig**.

Hinweis: Nach dem Schutz eines Netzwerks erinnert das Dialogfenster "Ihr nächster Schritt" daran, dass Sie Wireless Network Security auf allen drahtlosen Computern installieren müssen, damit diese sich am Netzwerk anmelden können.

Wenn Sie zuvor für Ihren Router oder Zugriffspunkt einen vorinstallierten Schlüssel manuell konfiguriert haben und keine Verbindung bestand, während Sie versuchten, den Router oder Zugriffspunkt zu schützen, müssen Sie den Schlüssel auch in das Feld für den WEP-Schlüssel eingeben und auf "Verbinden" klicken. Wenn Sie zuvor den administrativen Benutzernamen oder das Kennwort geändert haben, erfolgt eine Aufforderung zur Eingabe dieser Informationen, bevor ein Router oder Zugriffspunkt geschützt wird.

Verwandte Themen

- Schutz anderer drahtloser Geräte (Seite 317)
- Computer zum geschützten drahtlosen Netzwerk hinzufügen (Seite 319)

An geschützten drahtlosen Netzwerken anmelden

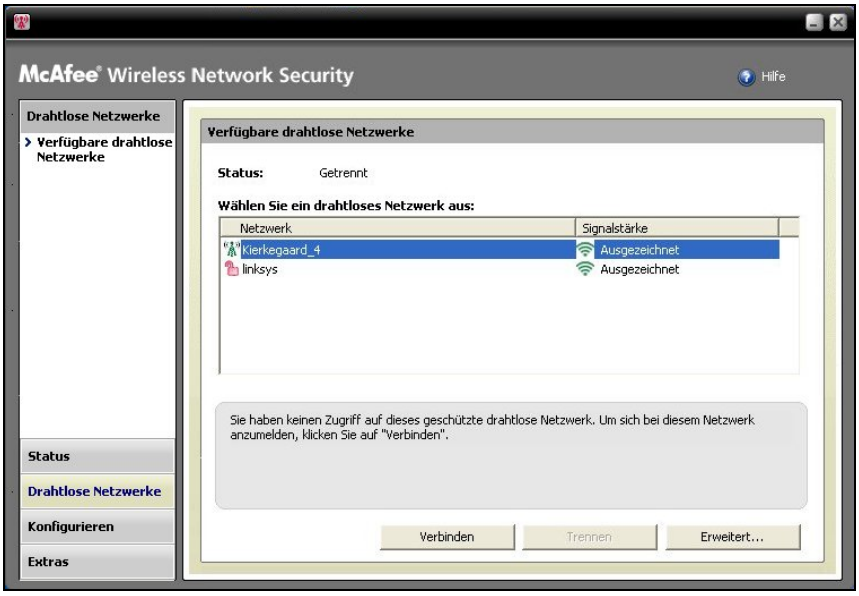
Ein geschütztes Netzwerk verhindert, dass Hacker Daten abfangen, die über das Netzwerk übertragen werden, und eine Verbindung zu Ihrem Netzwerk herstellen. Bevor ein berechtigter Computer auf ein geschütztes drahtloses Netzwerk zugreifen kann, muss dieser zunächst angemeldet werden.

Wenn ein Computer die Anmeldung zu einem verwalteten Netzwerk anfragt, wird eine Nachricht an die anderen Computer des Netzwerks gesendet, die über administrative Zugriffsrechte verfügen. Als Administrator sind Sie dafür zuständig, zu entscheiden, welche Art von Zugriffsrecht einem Computer gewährt wird: als Gast, vollständig oder administrativ.

Bevor Sie sich an einem geschützten Netzwerk anmelden können, müssen Sie Wireless Network Security installieren und dann eine Verbindung zum geschützten drahtlosen Netzwerk aufbauen. Ein bestehender Netzwerkbenutzer, der über administrative Zugriffsrechte auf das geschützte drahtlose Netzwerk verfügt, muss Ihre Anmeldung zum Netzwerk genehmigen. Nach der Anmeldung zum Netzwerk ist bei einem Neuaufbau der Verbindung keine Neuanmeldung erforderlich. Sowohl der Rechtegewährer als auch der sich Anmeldende müssen über eine aktive drahtlose Verbindung verfügen. Der Rechtegewährer muss ein Administratorcomputer sein, der mit dem Netzwerk verbunden ist.

So melden Sie sich an einem geschützten drahtlosen Netzwerk an:

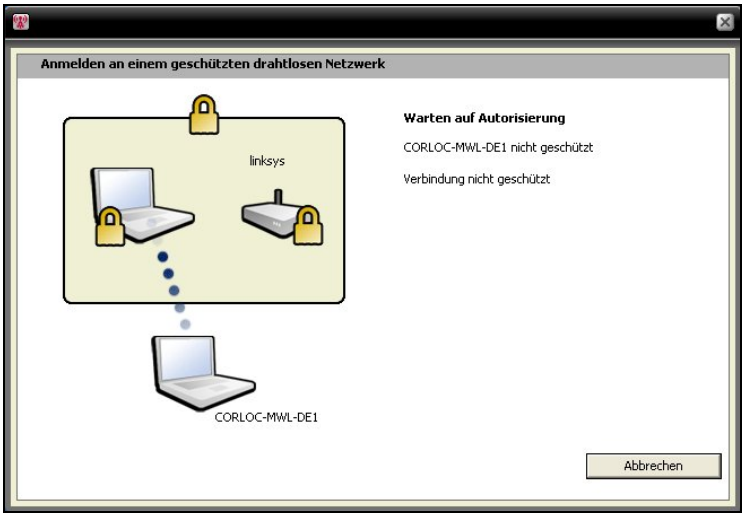
1. Klicken Sie auf dem ungeschützten Computer mit der rechten Maustaste auf das Symbol für Wireless Network Security im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Drahtlose Netzwerke anzeigen** aus.
3. Wählen Sie im Bereich "Verfügbare drahtlose Netzwerke" ein Netzwerk aus und klicken Sie auf **Verbinden**.



4 Klicken Sie im Dialogfenster "Beim geschützten drahtlosen Netzwerk anmelden" auf **Ja**, um sich am Netzwerk anzumelden.

Beim geschützten drahtlosen Netzwerk anmelden
Das Netzwerk Kierkegaard_4 wird von McAfee Wireless Network Security geschützt.
Um sich bei diesem Netzwerk anzumelden, klicken Sie auf "Ja".
Ja
Nein

Während Wireless Network Security versucht, die Genehmigung für die Anmeldung zum Netzwerk zu erhalten, erscheint das Fenster "Anmelden an einem geschützten drahtlosen Netzwerk" auf dem Computer, der versucht, sich am Netzwerk anzumelden.



5 Auf dem Administratorcomputer, über den die Gast-, vollständigen und administrativen Zugriffsrechte gewährt werden, erscheint das Fenster "Am Netzwerk anmelden".

Achtung! Ein Computer möchte sich am Netzwerk anmelden.
Verwaltetes Netzwerk - linksys
CORLOC_JIXP versucht, sich am Netzwerk linksys anzumelden.
Wenn Sie diesen Computer nicht kennen, empfehlen wir Ihnen, auf Anfrage ignorieren zu klicken. Wählen Sie anderenfalls den zu autorisierenden Zugriffstyp aus, und klicken Sie auf Zugriff gewähren .
CORLOC_JIXP den folgenden Zugriff gewähren:
Zugriff als Gast gewähren
Vollständigen Zugriff auf alle verwalteten Netzwerkanwendungen gewähren
Administrativen Zugriff auf alle verwalteten Netzwerkanwendungen gewähren
Hilfe
Zugriff gewähren
Anfrage ignorieren

Wählen Sie im Dialogfenster "Am Netzwerk anmelden" eine der folgenden Optionen aus:

Zugriff als Gast gewähren	Diese Option erlaubt dem Computer, Dateien an andere auf dem drahtlosen Netzwerk befindliche Computer zu senden. Der Datenaustausch mit McAfee EasyNetwork ist nicht möglich.
Vollständigen Zugriff auf alle verwalteten Netzwerk-anwendungen gewähren	Diese Option erlaubt dem Computer den Datenversand an und den Datenaustausch mit McAfee EasyNetwork.
Administrativen Zugriff auf alle verwalteten Netzwerk-anwendungen gewähren:	Diese Option erlaubt dem Computer den Datenversand an und den Datenaustausch mit McAfee EasyNetwork, die Erteilung von Zugriffsrechten für andere Computer und die Anpassung der Zugriffsstufen der anderen Computer auf dem drahtlosen Netzwerk.

6 Klicken Sie auf **Zugriff gewähren**.

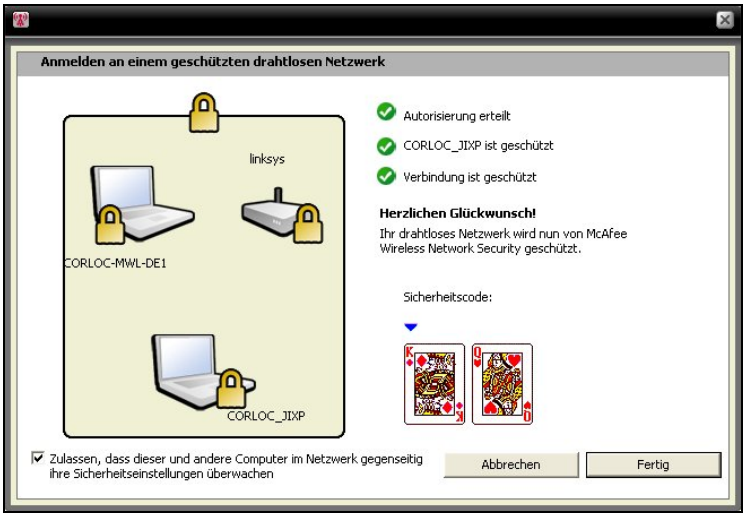
7 Bestätigen Sie, dass die im Bereich "Gewähren von Netzwerkzugriff" angezeigten Karten denen auf dem Computer angezeigten entsprechen, der versucht, sich am drahtlosen Netzwerk anzumelden. Sollten die Karten übereinstimmen, klicken Sie auf **Zugriff gewähren**.

Sollten die Computer nicht die gleichen Spielkarten anzeigen, liegt möglicherweise ein Sicherheitsverstoß vor. Diesem

Computer Zugriffsrechte zum Netzwerk zu gewähren, kann ein Risiko für Ihren Computer darstellen. Um dem Computer den Zugriff auf das drahtlose Netzwerk zu untersagen, klicken Sie auf **Zugriff verweigern**.

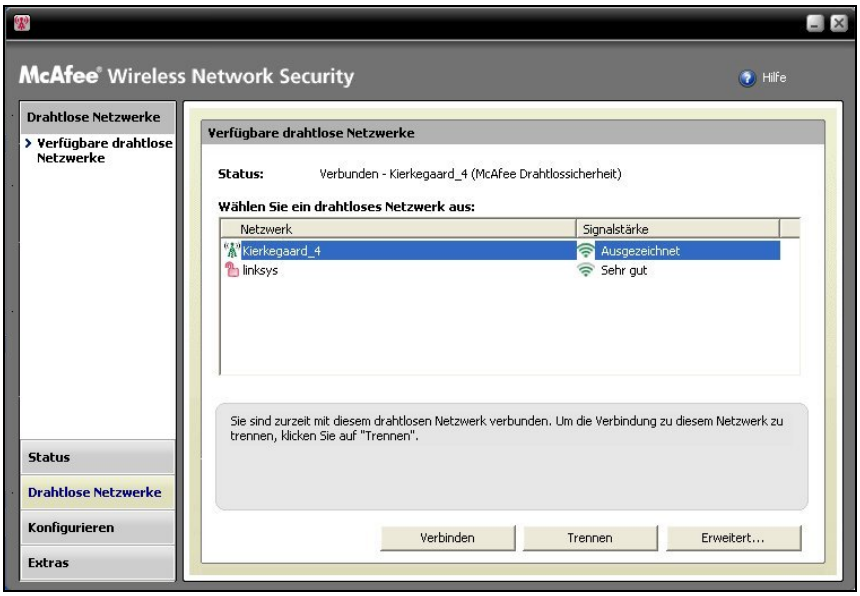
Gewähren von Netzwerkzugriff...
Verwaltetes Netzwerk - Kierkegaard_1
Aus Sicherheitsgründen...
Bestätigen Sie, dass die folgenden Karten von CORLOC-MWL-DE2 gesehen werden können, um das Gewähren des Zugriffs abzuschließen:
Hilfe
Zugriff gewähren
Zugriff verweigern

8 Der Bereich "Gewähren von Netzwerkzugriff" bestätigt, dass der neue Computer durch Wireless Network Security geschützt ist. Um die Sicherheitseinstellungen von anderen Computern zu überwachen und den anderen Computern zu erlauben, die Sicherheitseinstellungen Ihres Computers zu überwachen, wählen Sie **Es diesem und anderen Computern erlauben, gegenseitig ihre Sicherheitseinstellungen zu überwachen** aus.



9 Klicken Sie auf **Fertig**.

10 Der Bereich "Verfügbare drahtlose Netzwerke" zeigt an, dass Sie mit dem geschützten drahtlosen Netzwerk verbunden sind.



Verwandte Themen

- Computer zum geschützten drahtlosen Netzwerk hinzufügen (Seite 319)

Verbindung zu geschützten drahtlosen Netzwerken

Wenn Sie sich bereits an einem geschützten drahtlosen Netzwerk angemeldet und später die Verbindung abgebrochen haben und der Zugriff nicht widerrufen wurde, können Sie die Verbindung jederzeit wieder herstellen, ohne sich neu anmelden zu müssen.

So stellen Sie eine Verbindung zu einem geschützten drahtlosen Netzwerk her:

1 Klicken Sie mit der rechten Maustaste auf das Symbol für Wireless Network Security im Windows-Benachrichtigungsbereich.

2 Wählen Sie **Drahtlose Netzwerke anzeigen** aus.

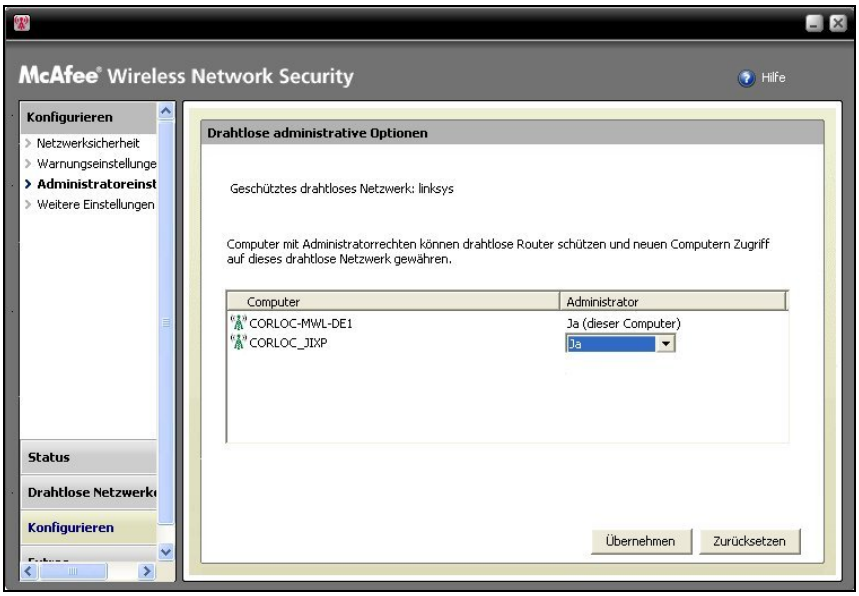
3 Wählen Sie im Bereich "Verfügbare drahtlose Netzwerke" ein Netzwerk aus, und klicken Sie auf **Verbinden**.

Computern administrativen Zugriff gewähren

Computer mit Administratorrechten können drahtlose Router schützen, Sicherheitsmodi ändern und neuen Computern Zugriff auf das geschützte drahtlose Netzwerk gewähren.

So konfigurieren Sie administrativen Zugriff:

1. Klicken Sie mit der rechten Maustaste auf das Symbol für Wireless Network Security im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Konfigurieren anzeigen** aus.
3. Wählen Sie im Bereich "Konfigurieren" **Administratoreinstellungen** aus.
4. Wählen Sie im Bereich "Drahtlose Administratorrechte" **Ja** oder **Nein** aus, um administrativen Zugriff zu gewähren oder abzulehnen.



5. Klicken Sie auf **Übernehmen**.

Verwandte Themen

- Über Zugriffstypen (Seite 307)
- Netzwerkzugriffsrechte aufheben (Seite 335)

Schutz anderer drahtloser Geräte

Über Wireless Network Security können Sie andere drahtlose Geräte zum Netzwerk hinzufügen. Hierzu gehören: drahtlose Drucker, Druckserver oder Spielekonsolen.

So fügen Sie andere drahtlose Geräte hinzu:

1. Klicken Sie mit der rechten Maustaste auf das Symbol für Wireless Network Security im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Tools anzeigen** aus.
3. Klicken Sie im Bereich "Sicherheitstools" unter **Nicht-AP-Geräte schützen** auf **Schützen**.
4. Wählen Sie im Bereich "Drahtloses Gerät" ein drahtloses Gerät aus und klicken Sie auf **Schützen**.
5. Die Meldung "Gerät ohne Zugriffspunkt geschützt" bestätigt, dass das Gerät zum Netzwerk hinzugefügt wurde.

Verbindung zu Netzwerken mit deaktivierter SSID-Übertragung

Sie können eine Verbindung zu drahtlosen Netzwerken aufbauen, bei denen SSID-Übertragung deaktiviert ist. Router, bei denen SSID-Übertragung deaktiviert ist, erscheinen nicht im Bereich "Verfügbare drahtlose Netzwerke".

McAfee empfiehlt, dass Sie drahtlose Router, bei denen SSID-Übertragung deaktiviert ist, nicht mit Wireless Network Security schützen.

So stellen Sie eine Verbindung zu einem drahtlosen Netzwerk her, bei dem SSID-Übertragung deaktiviert ist:

1. Klicken Sie mit der rechten Maustaste auf das Symbol für Wireless Network Security im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Drahtlose Netzwerke anzeigen** aus.
3. Klicken Sie im Bereich "Verfügbare drahtlose Netzwerke" auf **Erweitert**.
4. Klicken Sie im Bereich "Drahtlose Netzwerke" auf **Hinzufügen**.
5. Legen Sie im Bereich "Drahtloses Netzwerk hinzufügen" die folgenden Einstellungen fest, und klicken Sie auf **OK**:

Einstellung	Beschreibung
Netzwerk	Der Name Ihres Netzwerks. Bei der Modifikation eines Netzwerks kann der Name nicht geändert werden.
Sicherheitseinstellungen	Die Sicherheit für Ihr ungeschütztes Netzwerk. Beachten Sie, dass, wenn der drahtlose Adapter den von Ihnen ausgewählten Modus nicht unterstützt, eine Verbindung nicht möglich ist. Zu den Sicherheitsmodi gehören: Deaktiviert, Open WEP, Shared WEP, Auto WEP, WPA-PSK, WPA2-PSK.
Verschlüsselungsmodus	Die zum ausgewählten Sicherheitsmodus gehörende Verschlüsselung. Zu den Verschlüsselungsmodi gehören: WEP, TKIP, AES und TKIP+AES.

Hinweis: McAfee empfiehlt, dass Sie drahtlose Router, bei denen SSID-Übertragung deaktiviert ist, nicht mit Wireless Network Security schützen. Wenn Sie diese Funktion verwenden müssen, tun Sie dies ausschließlich, wenn SSID-Übertragung deaktiviert ist.

Computer zum geschützten drahtlosen Netzwerk hinzufügen

Computer können zum geschützten drahtlosen Netzwerk mithilfe eines Wechselgeräts, wie beispielsweise USB-Flash-Laufwerk, beschreibbare CD oder die Windows Connect Now-Technologie, hinzugefügt werden.

Hinzufügen von Computern über Wechselgeräte

Über Wireless Network Security können Sie zusätzliche Computer, auf denen kein Wireless Network Security läuft, über ein USB-Flash-Laufwerk oder eine beschreibbare CD zum geschützten drahtlosen Netzwerk hinzufügen.

So fügen Sie einen Computer hinzu:

1. Klicken Sie mit der rechten Maustaste auf das Symbol für Wireless Network Security im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Tools anzeigen** aus.
3. Klicken Sie im Bereich "Sicherheitstools" unter **Computer schützen** auf **Schützen**.
4. Wählen Sie im Bereich "Anderen Computer schützen" **Kopieren Sie Wireless Network Security auf ein Wechselgerät, wie einen USB-Schlüssel** aus.

Anderen Computer schützen
Um einen anderen Computer zu schützen, auf dem Wireless Network Security ausgeführt wird, klicken Sie auf Hilfe.
Wenn der Computer nicht durch Wireless Network Security geschützt wird, führen Sie eine der folgenden Aktionen aus:
Kopieren Sie Wireless Network Security auf ein Wechselgerät, wie einen USB-Schlüssel.
Erstellen Sie eine Windows ConnectNow-Disk.
Speicherort auswählen:
USB MEMORY (H:)
Hilfe
Kopieren
Abbrechen

5 Wählen Sie den Ort des CD- oder des USB-Flash-Laufwerks, auf das Wireless Network Security kopiert werden soll.

6 Klicken Sie auf **Kopieren**.

7 Nachdem alle Dateien auf das CD- oder USB-Flash-Laufwerk kopiert wurden, legen Sie das Wechselgerät in den Computer ein, der geschützt werden soll. Sollte das Programm nicht automatisch starten, durchsuchen Sie den Inhalt des Wechselmediums über den Windows Explorer und klicken Sie auf **Install.exe**.

8 Befolgen Sie die Anweisungen auf dem Bildschirm.

Hinweis: Weiterhin können Sie mithilfe der Windows Connect Now-Technologie einen Computer zum geschützten drahtlosen Netzwerk hinzufügen.

Verwandte Themen

- Hinzufügen von Computern mithilfe der Windows Connect Now-Technologie (Seite 321)

Hinzufügen von Computern mithilfe der Windows Connect Now-Technologie

Über Wireless Network Security können Sie zusätzliche Computer, auf denen Wireless Network Security nicht ausgeführt wird, über die Windows Connect Now-Technologie hinzufügen.

So fügen Sie einen Computer mithilfe der Windows Connect Now-Technologie hinzu:

1. Klicken Sie mit der rechten Maustaste auf das Symbol für Wireless Network Security im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Tools anzeigen** aus.
3. Klicken Sie im Bereich "Sicherheitstools" unter **Computer schützen** auf **Schützen**.
4. Wählen Sie im Bereich "Anderen Computer schützen" **Windows Connect Now-Disk erstellen** aus.
5. Wählen Sie einen Speicherort für die Kopie der Windows Connect Now-Informationen.
6. Klicken Sie auf **Kopieren**.
7. Legen Sie die Windows Connect Now-Disk in den Computer ein, den Sie schützen möchten.
8. Führen Sie eine der folgenden Aktionen durch, wenn die Disk nicht automatisch starten sollte:
   - Installieren Sie die Wireless Connect Now-Technologie: Klicken Sie auf der Windows-Taskleiste auf **Start** und dann auf **Systemsteuerung**. Wenn Sie die Kategorieansicht der Systemsteuerung verwenden, klicken Sie auf **Netzwerk- und Internetverbindungen** und dann auf den **Assistent für die Einrichtung drahtloser Netzwerke**. Wenn Sie die klassische Ansicht der Systemsteuerung verwenden, klicken Sie auf **Assistent für die Einrichtung drahtloser Netzwerke**. Befolgen Sie die Anweisungen auf dem Bildschirm.
   - Öffnen Sie die Datei `setupSNK.exe` auf der Windows Connect-Disk, kopieren Sie den Schlüssel und fügen Sie diesen in den Auswahlclient Ihres drahtlosen Netzwerks ein.

Hinweis: Setzen Sie die Schlüsselrotation aus, wenn Sie die Windows Connect Now-Technologie für die Verbindung zum drahtlosen Netzwerk verwenden. Anderenfalls schlägt die Netzwerkverbindung fehl. Die Verbindung schlägt fehl, da die Schlüsselrotation einen neuen Schlüssel erstellt, der sich vom Schlüssel, den die Windows Connect Now-Technologie verwendet, unterscheidet.

Computer können zum geschützten drahtlosen Netzwerk weiterhin mithilfe eines Wechselgeräts, wie beispielsweise eine beschreibbare CD oder ein USB-Flash-Laufwerk, hinzugefügt werden.

Verwandte Themen

- Hinzufügen von Computern über Wechselgeräte (Seite 319)

KAPITEL 42

Drahtlosen Netzwerken verwalten

Wireless Network Security bietet einen vollständigen Satz an Administratortools für die Verwaltung und Pflege Ihres drahtlosen Netzwerks.

In diesem Kapitel

Verwalten drahtloser Netzwerke.....324

Verwalten drahtloser Netzwerke

Wenn Sie mit einem geschützten drahtlosen Netzwerk verbunden sind, werden die gesendeten und empfangenen Informationen verschlüsselt. Hacker können die im geschützten Netzwerk übertragenen Daten nicht entschlüsseln und auch keine Verbindung zu Ihrem Netzwerk herstellen. Wireless Network Security bietet eine Vielzahl von Tools, die Ihnen bei der Verwaltung Ihres Netzwerks behilflich sind, um weitere Intrusionen zu verhindern.

Über Wireless Network Security-Symbole

Wireless Network Security zeigt Symbole an, um diverse Netzwerkverbindungstypen und Signalstärken darzustellen.

Netzwerkverbindungssymbole

Die folgende Tabelle beschreibt die Symbole, die in Wireless Network Security in den Bereichen "Status des drahtlosen Netzwerks", "Sicherheitstools" und "Verfügbare drahtlose Netzwerke" zum Einsatz kommen. Die Symbole stellen diverse Netzwerkverbindungs- und Sicherheitsstatus dar.

Symbol	Statusbereiche	Schutzbereiche
	Ihr Computer ist mit dem ausgewählten geschützten drahtlosen Netzwerk verbunden.	Das Gerät ist durch Wireless Network Security geschützt.
	Ihr Computer kann auf das geschützte drahtlose Netzwerk zugreifen, aber ist derzeit nicht damit verbunden.	Das Gerät verwendet WEP- oder WPA-Sicherheit.
	Ihr Computer ist ein ehemaliges Mitglied des geschützten drahtlosen Netzwerks, aber das Zugriffsrecht wurde widerrufen, als die Verbindung des Computers mit dem Netzwerk aufgehoben wurde.	Für das Gerät ist Wireless Network Security deaktiviert.

Signalstärkensymbole

Die folgende Tabelle beschreibt die Symbole, die von Wireless Network Security für die Darstellung diverser Netzwerksignalstärken verwendet werden.

Symbol	Beschreibung
	Ausgezeichnete Signalstärke
	Sehr gute Signalstärke
	Gute Signalstärke
	Niedrige Signalstärke

Verwandte Themen

- Signalstärke des Netzwerks ansehen (Seite 358)
- Derzeit geschützte Computer ansehen (Seite 364)
- Netzwerksicherheitsmodus ansehen (Seite 356)

Bevorzugte Netzwerke auflisten

Über Wireless Network Security können Sie bevorzugte drahtlose Netzwerke festlegen. Hierüber können Sie die Reihenfolge der Netzwerke angeben, zu denen Ihr Computer automatisch eine Verbindung aufbaut. Wireless Network Security versucht zum ersten Netzwerk auf der Liste eine Verbindung aufzubauen.

Diese Funktion ist hilfreich, wenn Sie beispielsweise automatisch eine Verbindung zum drahtlosen Netzwerk eines Freundes aufbauen möchten, wenn Sie sich in der Nähe befinden. Sie können ein anderes Netzwerk auf den ersten Listenplatz setzen.

So listen Sie bevorzugte Netzwerke auf:

1. Klicken Sie mit der rechten Maustaste auf das Symbol für Wireless Network Security im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Drahtlose Netzwerke anzeigen** aus.
3. Klicken Sie im Bereich "Verfügbare drahtlose Netzwerke" auf **Erweitert**.
4. Wählen Sie das Netzwerk aus, dessen Listenplatz Sie anpassen möchten und klicken Sie auf **Nach oben** oder **Nach unten**.

5. Klicken Sie auf **OK**.

Verwandte Themen

- Bevorzugte drahtlose Netzwerke entfernen (Seite 327)

Bevorzugte drahtlose Netzwerke entfernen

Über Wireless Network Security können Sie bevorzugte Netzwerke entfernen.

Dies ist hilfreich, wenn Sie beispielsweise ein überflüssiges Netzwerk aus der Liste streichen möchten.

So entfernen Sie bevorzugte Netzwerke:

1. Klicken Sie mit der rechten Maustaste auf das Symbol für Wireless Network Security im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Drahtlose Netzwerke anzeigen** aus.
3. Klicken Sie im Bereich "Verfügbare drahtlose Netzwerke" auf **Erweitert**.
4. Wählen Sie im Bereich "Verfügbare drahtlose Netzwerke" ein Netzwerk aus, und klicken Sie auf **Entfernen**.
5. Klicken Sie auf **OK**.

Verwandte Themen

- Bevorzugte Netzwerke auflisten (Seite 326)

Geschützte drahtlose Netzwerke umbenennen

Über Wireless Network Security können Sie ein bestehendes geschütztes drahtloses Netzwerk umbenennen.

Das Umbenennen eines Netzwerks kann hilfreich sein, wenn beispielsweise Ihr Nachbar einen ähnlichen oder gleichen Namen verwendet, oder wenn Sie einen unverwechselbaren Namen erstellen möchten.

Computer, die mit dem geschützten drahtlosen Netzwerk verbunden sind, müssen möglicherweise eine manuelle Wiederherstellung der Verbindung durchführen und werden benachrichtigt, wenn sich der Name ändert.

Nach der Umbenennung des Netzwerks erscheint der Name im Bereich "Geschützter drahtloser Router/Zugriffspunkt".

So ändern Sie den Namen Ihres geschützten drahtlosen Netzwerks:

1. Klicken Sie mit der rechten Maustaste auf das Symbol für Wireless Network Security im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Konfigurieren anzeigen** aus.
3. Geben Sie den neuen Namen im Bereich "Netzwerksicherheit" in das Feld **Name des geschützten drahtlosen Netzwerks** ein.
4. Klicken Sie auf **Übernehmen**.

   Das Dialogfenster "Netzwerk-Sicherheitseinstellungen werden aktualisiert" wird angezeigt, während Wireless Network Security den Namen des geschützten drahtlosen Netzwerks ändert. In Abhängigkeit von den Einstellungen Ihres Computers und der Signalstärke dauert die Namensänderung für das Netzwerk weniger als eine Minute.

Hinweis: Als Sicherheitsmaßnahme empfiehlt McAfee, dass Sie die Standard-SSID des Routers oder des Zugriffspunkts umbenennen. Obwohl Wireless Network Security Standard-SSIDs, wie beispielsweise "linksys" oder "belkin54g" oder "NETGEAR" unterstützt, schützt das Umbenennen der SSIDs vor Zugriffspunktbedrohungen.

Warneinstellungen konfigurieren

Über Wireless Network Security können Sie Warneinstellungen konfigurieren, um Warnungen anzeigen zu lassen, wenn bestimmte Ereignisse auftreten, wie beispielsweise der Verbindungsaufbau eines neuen Computers zum Netzwerk.

So konfigurieren Sie Warnverhalten:

1. Klicken Sie mit der rechten Maustaste auf das Symbol für Wireless Network Security im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Konfigurieren anzeigen** aus.
3. Klicken Sie auf **Warneinstellungen**.
4. Wählen Sie eines oder mehrere der folgenden Ereignisse aus, oder entfernen Sie die Markierung, und klicken Sie auf **Übernehmen**:

Warnungseinstellung	Beschreibung
Der Sicherheitsschlüssel für Ihr geschütztes drahtloses Netzwerk wird rotiert.	Zeigt die Meldung "Sicherheitsschlüssel rotiert" an, nachdem der Sicherheitsschlüssel manuell oder automatisch rotiert wurde. Das Rotieren des Schlüssels schützt das Netzwerk vor Hackern, die versuchen, Ihre Daten abzufangen oder eine Verbindung zu Ihrem Netzwerk aufzubauen.
Ein anderer geschützter Computer stellt eine Verbindung zum Netzwerk her oder trennt eine Verbindung.	Zeigt die Meldungen "Computer verbunden" oder "Computer getrennt" an, nachdem ein Computer eine Verbindung zu einem geschützten drahtlosen Netzwerk aufgebaut oder getrennt hat. Die Daten auf verbundenen Computern sind jetzt gegen Intrusionen und Datenabfang geschützt.
Einem anderen Computer wird Zugriff auf Ihr geschütztes drahtloses Netzwerk gewährt.	Zeigt die Meldung "Computer hat Netzwerkzugriff gewährt" an, nachdem ein Administratorcomputer einem anderen Computer die Anmeldung zum geschützten drahtlosen Netzwerk gewährt hat. Einem Computer den Zugriff auf das geschützte Netzwerk zu gewähren, schützt vor Hackern, die versuchen, Ihre Daten abzufangen.
Die Schlüsselrotation für Ihr geschütztes drahtloses Netzwerk wird ausgesetzt oder wieder aufgenommen.	Zeigt entweder die Meldung "Schlüsselrotation ausgesetzt" oder "Schlüsselrotation fortgesetzt" an, nachdem Sie manuell die Schlüsselrotation ausgesetzt oder wieder aufgenommen haben. Das Rotieren des Schlüssels schützt das Netzwerk vor Hackern, die versuchen, Ihre Daten abzufangen oder eine Verbindung zu Ihrem Netzwerk aufzubauen.
Der Zugriff aller nicht verbundenen Computer wird widerrufen.	Zeigt die Meldung "Zugriff widerrufen" an, nachdem der Zugriff für Computer, die nicht mit dem Netzwerk verbunden sind, widerrufen wurde. Computer, deren Verbindung unterbrochen wurde, müssen sich erneut am Netzwerk anmelden.
Ein Router wurde zu Ihrem geschützten drahtlosen Netzwerk hinzugefügt oder daraus entfernt.	Zeigt die Meldungen "Router/Zugriffspunkt zum Netzwerk hinzugefügt" oder "Router/Zugriffspunkt ungeschützt" an, nachdem der Router oder der Zugriffspunkt zum geschützten drahtlosen Netzwerk hinzugefügt oder davon entfernt wurde.

Warnungseinstellung	Beschreibung
Die Anmeldeinformationen für einen geschützten drahtlosen Router wurden geändert.	Zeigt die Meldung "Anmeldeinformationen für Router/Zugriffspunkt geändert" an, nachdem der Wireless Network Security-Administrator den Benutzernamen oder das Kennwort eines Routers oder Zugriffspunkts geändert hat.
Der Name oder eine Sicherheitseinstellung Ihres geschützten drahtlosen Netzwerks wurde geändert.	Zeigt die Meldungen "Netzwerkeinstellungen geändert" oder "Netzwerk umbenannt" an, nachdem Sie das geschützte drahtlose Netzwerk umbenannt oder deren Sicherheitseinstellungen angepasst haben.
Die Einstellungen für Ihr geschütztes drahtloses Netzwerk werden repariert.	Zeigt die Meldung "Netzwerk repariert" an, nachdem Probleme in Bezug auf die Sicherheitseinstellungen auf den drahtlosen Routern oder Zugriffspunkten Ihres Netzwerks behoben wurden.

Hinweis: Um alle Warnmeldungen auszuwählen oder zu löschen, wählen Sie **Alles markieren** oder **Alles löschen**. Um die Warneinstellungen von Wireless Network Security zurückzusetzen, klicken Sie auf **Standardwerte wiederherstellen**.

Verwandte Themen

- Schlüssel automatisch rotieren (Seite 345)
- Anmelden an einem geschützten drahtlosen Netzwerk (Seite 310)
- Verbindung zu geschützten drahtlosen Netzwerken (Seite 315)
- Verbindung zum geschützten drahtlosen Netzwerk aufheben (Seite 334)
- Automatische Schlüsselrotation aussetzen (Seite 348)
- Netzwerkzugriffsrechte aufheben (Seite 335)
- Drahtlose Router oder Zugriffspunkte entfernen (Seite 333)
- Informationen für drahtlose Geräte ändern (Seite 341)
- Geschützte drahtlose Netzwerke umbenennen (Seite 328)
- Netzwerk-Sicherheitseinstellungen reparieren (Seite 342)

Verbindungsbenachrichtigung anzeigen

Sie können Wireless Network Security so einrichten, dass Sie eine Benachrichtigung erhalten, wenn Ihr Computer eine Verbindung mit einem drahtlosen Netzwerk aufbaut.

So lassen Sie die Benachrichtigung anzeigen, wenn eine Verbindung zu einem drahtlosen Netzwerk aufgebaut wird:

1. Klicken Sie mit der rechten Maustaste auf das Symbol für Wireless Network Security im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Konfigurieren anzeigen** aus.
3. Klicken Sie auf **Weitere Einstellungen**.
4. Wählen Sie **Bei einer Verbindung mit einem drahtlosen Netzwerk benachrichtigen** aus.
5. Klicken Sie auf **Übernehmen**.

Verwandte Themen

- Verbindung zu geschützten drahtlosen Netzwerken (Seite 315)

Drahtlose Router oder Zugriffspunkte entfernen

Über Wireless Network Security können Sie einen oder mehrere Router oder Zugriffspunkte von Ihrem geschützten Netzwerk entfernen.

So entfernen Sie einen drahtlosen Router oder Zugriffspunkt:

1. Klicken Sie mit der rechten Maustaste auf das Symbol für Wireless Network Security im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Tools anzeigen** aus.
3. Klicken Sie im Bereich "Sicherheitstools" unter **Den Schutz für ein Gerät aufheben** auf **Schutz aufheben**.
4. Wählen Sie im Bereich "Schutz für drahtlosen Router/Zugriffspunkt aufheben" einen drahtlosen Router oder Zugriffspunkt aus, der vom geschützten Netzwerk entfernt werden soll, und klicken Sie auf **Schutz aufheben**.

Schutz für drahtlosen Router/Zugriffspunkt aufheben
Wählen Sie einen drahtlosen Router oder Zugriffspunkt aus, der aus Ihrem geschützten Netzwerk entfernt werden soll.
Drahtloser Router oder Zugriffspunkt
Netzwerk
Linksys WRT54G (192.168.1.1)
Kierkegaard_1
Aktualisieren
Dieser drahtlose Router oder Zugriffspunkt ist derzeit geschützt. Klicken Sie zum Aufheben des Schutzes auf "Schutz aufheben".
Schutz aufheben
Abbrechen
Hilfe

5. Klicken Sie im Dialogfeld "Drahtloser Router/Zugriffspunkt ungeschützt" auf **OK**, um zu bestätigen, dass der Router oder der Zugriffspunkt vom Netzwerk entfernt wurde.

Verwandte Themen

- Geschützte drahtlose Netzwerke erstellen (Seite 308)

Verbindung zum geschützten drahtlosen Netzwerk aufheben

Über Wireless Network Security können Sie die Verbindung Ihres Computers zum Netzwerk aufheben.

Diese Funktion ist hilfreich, wenn Ihr Computer beispielsweise eine Verbindung zu einem Netzwerk unter Verwendung eines Namens aufgebaut hat, der mit dem Netzwerknamen übereinstimmt. Sie können die Verbindung zum Netzwerk aufheben und dann eine erneute Verbindung zu Ihrem Netzwerk herstellen.

Diese Funktion ist hilfreich, wenn Sie aus Versehen aufgrund einer hohen Signalstärke eines anderen Zugriffspunkts oder einer Funktionsstörung eine Verbindung zu einem falschen Netzwerk aufgebaut haben.

So heben Sie eine Verbindung zu einem geschützten drahtlosen Netzwerk auf:

1. Klicken Sie mit der rechten Maustaste auf das Symbol für Wireless Network Security im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Drahtlose Netzwerke anzeigen** aus.
3. Wählen Sie im Bereich "Verfügbare drahtlose Netzwerke" ein Netzwerk aus und klicken Sie auf **Trennen**.

Verwandte Themen

- Netzwerkzugriffsrechte aufheben (Seite 335)
- Geschützte drahtlose Netzwerke verlassen (Seite 336)

Netzwerkzugriffsrechte aufheben

Über Wireless Network Security können Sie den Zugriff von Computern ablehnen, die nicht mit dem Netzwerk verbunden sind. Es wird ein neuer Rotationsplan für den Sicherheitsschlüssel aufgestellt: Computer, die nicht verbunden sind, verlieren den Zugriff auf das geschützte drahtlose Netzwerk, aber können den Zugriff wieder erlangen, wenn Sie sich erneut am Netzwerk anmelden. Der Zugriff verbundener Computer wird aufrechterhalten.

Beispielsweise können Sie den Zugriff eines Besuchercomputer mit Wireless Network Security widerrufen, nachdem diese die Verbindung getrennt hat. Zusätzlich kann ein Erwachsener aus Jugendschutzgründen den Zugriff eines Computers, der von einem Kind verwendet wird, widerrufen. Ein zuvor versehentlich gewährter Zugriff kann ebenfalls widerrufen werden.

So widerrufen Sie den Zugriff aller Computer, deren Verbindung zum geschützten Netzwerk getrennt ist:

1. Klicken Sie mit der rechten Maustaste auf das Symbol für Wireless Network Security im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Tools anzeigen** aus.
3. Klicken Sie im Bereich "Extras" auf "Wartungstools".
4. Klicken Sie im Bereich "Wartungstools" unter **Zugriff widerrufen** auf **Widerrufen**.
5. Klicken Sie im Bereich "Zugriff widerrufen" auf **Widerrufen**.
6. Klicken Sie im Wireless Network Security-Dialogfeld auf **OK**.

Verwandte Themen

- Verbindung zum geschützten drahtlosen Netzwerk aufheben (Seite 334)
- Geschützte drahtlose Netzwerke verlassen (Seite 336)

Geschützte drahtlose Netzwerke verlassen

Sie können Wireless Network Security dazu verwenden, Ihre Zugriffrechte auf ein geschütztes Netzwerk abzubrechen.

So verlassen Sie ein Netzwerk:

1. Klicken Sie mit der rechten Maustaste auf das Symbol für Wireless Network Security im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Konfigurieren anzeigen** aus.
3. Wählen Sie im Bereich "Konfigurieren" **Weitere Einstellungen** aus.
4. Wählen Sie im Bereich "Weitere Einstellungen" unter "Zugriff auf geschütztes Netzwerk" das Netzwerk aus, das Sie verlassen möchten und klicken Sie auf **Netzwerk verlassen**.
5. Klicken Sie im Bereich "Verbindung zum Netzwerk trennen" auf **Ja**, um das Netzwerk zu verlassen.

Hinweis: Wenn Sie ein Netzwerk verlassen haben, muss Ihnen ein anderer Benutzer den Zugriff auf das geschützte Netzwerk wieder gewähren, bevor Sie sich erneut an diesem Netzwerk anmelden können.

Verwandte Themen

- Verbindung zum geschützten drahtlosen Netzwerk aufheben (Seite 334)
- Netzwerkzugriffsrechte aufheben (Seite 335)

KAPITEL 43

Sicherheit für drahtloses Netzwerk verwalten

Wireless Network Security bietet einen vollständigen Satz an Tools für die Verwaltung der Sicherheitsfunktionen Ihres drahtlosen Netzwerks.

In diesem Kapitel

Konfigurieren von Sicherheitseinstellungen.....338
Netzwerkschlüssel verwalten 343

Konfigurieren von Sicherheitseinstellungen

Nachdem Sie eine Verbindung zu einem geschützten drahtlosen Netzwerk aufgebaut haben, schützt Wireless Network Security automatisch Ihr Netzwerk. Allerdings können Sie jederzeit zusätzliche Sicherheitseinstellungen konfigurieren.

Sicherheitsmodi konfigurieren

Sie können den Sicherheitsmodus Ihres geschützten drahtlosen Netzwerks festlegen. Sicherheitsmodi definieren die Verschlüsselung zwischen Ihrem Computer und dem Router oder Zugriffspunkt.

Wenn Sie Ihr Netzwerk schützen, wird WEP automatisch konfiguriert. Allerdings empfiehlt McAfee, dass Sie den Sicherheitsmodus auf WPA2 oder WPA-PSK AES ändern. Wireless Network Security verwendet anfänglich WEP, da dieser Modus von allen Routern und Adaptern für drahtlose Netzwerke unterstützt wird. Die meisten neuen Router und Adapter für drahtlose Netzwerke arbeiten allerdings im WPA-Modus. Dieser ist sicherer.

So ändern Sie den Sicherheitsmodus für ein geschütztes drahtloses Netzwerk:

1. Klicken Sie mit der rechten Maustaste auf das Symbol für Wireless Network Security im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Konfigurieren anzeigen** aus.
3. Wählen Sie im Bereich "Netzwerksicherheit" im Feld **Sicherheitsmodus** die Sicherheitsmethode aus, die Sie verwenden möchten und klicken Sie auf **Übernehmen**.

Die folgende Tabelle beschreibt die verfügbaren Sicherheitsmodi:

Stärke	Modus	Beschreibung
Schwächste	WEP	Wired Equivalent Privacy (WEP) ist Teil der Norm IEEE 802.11 für drahtlose Netzwerke zur Sicherung von drahtlosen IEEE 802.11-Netzwerken. WEP bietet eine Sicherheitsstufe, die einen schwachen Versuch, in die Privatsphäre einzudringen, verhindern kann, aber nicht so sicher ist wie die WPA-PSK-Verschlüsselung. Obwohl Wireless Network Security einen starken (schwer zu erratenden und langen) Schlüssel erstellt, empfiehlt McAfee, dass Sie einen WPA-Sicherheitsmodus verwenden.
Durchschnittlich	WPA-PSK TKIP	Wi-Fi Protected Access (WPA) ist eine frühe Version des Sicherheitsstandards 802.11i. TKIP wurde für WPA entwickelt, um WEP zu verbessern. TKIP bietet Nachrichtenintegrität, Mechanismen zur Neuverteilung von Schlüsseln und Paketschlüsselmischung.
Stark	WPA-PSK AES	Dieser Sicherheitsmodus kombiniert WPA- und AES-Modi. Advanced Encryption Standard (AES) ist eine Blockchiffre, die von der US-Regierung als Verschlüsselungsstandard verwendet wird.
Stärkere	WPA2-PSK AES	Dieser Sicherheitsmodus kombiniert WPA2- und AES-Modi. WPA2 ist die nächste Erweiterung der Ratifizierung des Sicherheitsstandards 802.11i. WPA2 bindet Counter Mode CBC MAC Protocol (CCMP) ein. Diese Lösung ist sicherer und skalierbarer als TKIP. Hierbei handelt es sich um den stärksten Sicherheitsmodus, der Verbrauchern zur Verfügung steht.

Stärke	Modus	Beschreibung
Stärkste	WPA2-PSK TKIP+AES	Dieser Sicherheitsmodus kombiniert WPA2- und AES- als auch WPA-PSK TKIP-Modi. Hierbei ist eine größere Flexibilität möglich, so dass sowohl alte als auch neue drahtlose Adapter angeschlossen werden können.

Hinweis: Nach der Änderung des Sicherheitsmodus ist es möglicherweise notwendig, dass Sie erneut manuell eine Verbindung aufbauen.

Verwandte Themen

- Netzwerk-Sicherheitseinstellungen reparieren (Seite 342)
- Netzwerksicherheitsmodus ansehen (Seite 356)

Netzwerk-Sicherheitseinstellungen konfigurieren

Sie können die Netzwerkeinstellungen von Netzwerken, die durch Wireless Network Security geschützt sind, ändern. Dies ist beispielsweise hilfreich, wenn Sie die Sicherheit von WEP auf WPA aufrüsten möchten.

McAfee empfiehlt, dass Sie die Netzwerk-Sicherheitseinstellungen ändern, wenn Sie durch eine Meldung dazu aufgefordert werden.

So konfigurieren Sie die Eigenschaften eines ungeschützten Netzwerks:

1. Klicken Sie mit der rechten Maustaste auf das Symbol für Wireless Network Security im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Drahtlose Netzwerke anzeigen** aus.
3. Klicken Sie im Bereich "Verfügbare drahtlose Netzwerke" auf **Erweitert**.
4. Klicken Sie im Bereich "Drahtlose Netzwerke" auf **Eigenschaften**.
5. Ändern Sie im Bereich "Eigenschaften des drahtlosen Netzwerks" die folgenden Einstellungen, und klicken Sie auf **OK**:

Einstellung	Beschreibung
Netzwerk	Der Name Ihres Netzwerks. Bei der Modifikation eines Netzwerks kann der Name nicht geändert werden.

Einstellung	Beschreibung
Sicherheitseinstellungen	Die Sicherheit für Ihr ungeschütztes Netzwerk. Beachten Sie, dass wenn der drahtlose Adapter den von Ihnen ausgewählten Modus nicht unterstützt, eine Verbindung nicht möglich ist. Zu den Sicherheitsmodi gehören: Deaktiviert, Open WEP, Shared WEP, Auto WEP, WPA-PSK, WPA2-PSK.
Verschlüsselungsmodus	Die zum ausgewählten Sicherheitsmodus gehörende Verschlüsselung. Zu den Verschlüsselungsmodi gehören: WEP, TKIP, AES und TKIP+AES.

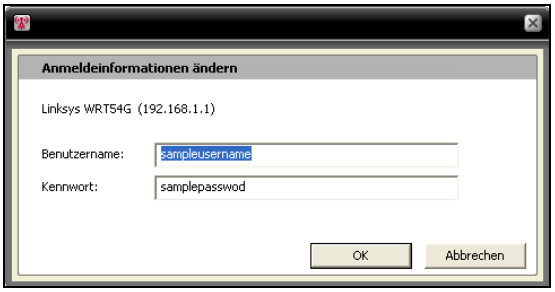
Informationen für drahtlose Geräte ändern

Sie können den Benutzernamen und das Kennwort für ein Gerät auf Ihrem geschützten drahtlosen Router oder Zugriffspunkt ändern. Die Liste der Geräte erscheint unter **Geschützte drahtlose Netzwerkgeräte**.

McAfee empfiehlt, dass Sie Ihre Anmeldeinformationen ändern, da die Mehrzahl der drahtlosen Geräte, die von einem Hersteller sind, dieselben Anmeldeinformationen aufweisen. Das Ändern der Anmeldeinformationen hilft zu verhindern, dass andere auf Ihren drahtlosen Router oder Zugriffspunkt zugreifen und Einstellungen ändern können.

So ändern Sie den Benutzernamen oder das Kennwort für ein geschütztes drahtloses Netzwerkgerät:

1. Klicken Sie mit der rechten Maustaste auf das Symbol für Wireless Network Security im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Konfigurieren anzeigen** aus.
3. Wählen Sie im Bereich "Netzwerksicherheit" unter **Geschützte drahtlose Netzwerkgeräte** einen drahtlosen Router oder Zugriffspunkt aus, und klicken Sie auf **Benutzernamen oder Kennwort ändern**.



4 Klicken Sie nach der Eingabe der Anmeldeinformationen im Dialogfenster "Wireless Network Security" auf **OK**.

Der neue Benutzername und das neue Kennwort erscheinen unter **Geschützte drahtlose Netzwerkgeräte**.

Hinweis: Einige Router unterstützen die Verwendung von Benutzernamen nicht. Daher erscheint kein Benutzername unter **Geschützte drahtlose Netzwerkgeräte**.

Netzwerk-Sicherheitseinstellungen reparieren

Wenn Sie Schwierigkeiten mit den Sicherheitseinstellungen oder der Konfiguration haben sollten, können Sie über Wireless Network Security die Einstellungen für Ihren Router oder Zugriffspunkt reparieren.

So reparieren Sie Ihre Sicherheitseinstellungen:

1 Klicken Sie mit der rechten Maustaste auf das Symbol für Wireless Network Security im Windows-Benachrichtigungsbereich.

2 Wählen Sie **Tools anzeigen** aus.

3 Klicken Sie im Bereich "Extras" auf **Wartungstools**.

4 Klicken Sie unter **Netzwerk-Sicherheitseinstellungen reparieren** auf **Reparieren**.

5 Klicken Sie im Bereich "Netzwerk-Sicherheitseinstellungen reparieren" auf **Reparieren**.

Eine Wireless Network Security-Meldung zeigt an, ob das Netzwerk repariert werden konnte oder nicht.

Hinweis: Sollte der Versuch, das Netzwerk zu reparieren, fehlschlagen, stellen Sie eine Verbindung zum Netzwerk über Kabel her, und versuchen Sie es erneut. Sollte sich das Kennwort für Router oder Zugriffspunkt geändert haben, müssen Sie das Kennwort neu eingeben, um eine Verbindung aufzubauen.

Netzwerkschlüssel verwalten

Wireless Network Security erstellt mithilfe eines Zufallsgenerators lange, starke und zufällige Verschlüsselungsschlüssel. Bei WEP wird der Schlüssel in einen hexadezimalen Wert mit 26 Zeichen übersetzt (für 104 Bits mittlerem Informationsgehalt oder Stärke, maximal durch 128-Bit-WEP unterstützte Stärke), während bei WPA der Schlüssel eine ASCII-Zeichenkette mit 63 Zeichen ist. Jedes Zeichen hat 64 mögliche Werte (6 Bits), wobei 384 Bits für den mittleren Informationsgehalt aufgebracht werden. Dies überschreitet die WAP-Schlüsselstärke von 256 Bits.

Bei der Verwaltung von Netzwerkschlüsseln können die Schlüssel als Klartext oder als Sternchen (für nicht geschützte Zugriffspunkte) angezeigt, gespeicherte Schlüssel für nicht geschützte Zugriffspunkte verworfen, Schlüsselrotation aktiviert oder deaktiviert, die Schlüsselrotationshäufigkeit geändert und die Schlüsselrotation ausgesetzt werden.

Bei einer automatischen Schlüsselrotation können die Tools der Hacker Ihre Daten nicht abfangen, da sich der Schlüssel fortwährend ändert.

Wenn Sie drahtlose Geräte, die von Wireless Network Security nicht unterstützt werden, mit dem Netzwerk verbinden (z. B. einen Handheld), müssen Sie den Schlüssel notieren, die Schlüsselrotation anhalten und den Schlüssel in das Gerät eingeben.

Aktuelle Schlüssel anzeigen

Wireless Network Security bietet einen schnellen Zugriff auf die drahtlosen Sicherheitsinformationen, einschließlich dem aktuellen Schlüssel für ein geschütztes drahtloses Netzwerk.

So lassen Sie den aktuellen Schlüssel anzeigen:

1. Klicken Sie mit der rechten Maustaste auf das Symbol "Wireless Network Security" im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Status anzeigen**.
3. Klicken Sie im Bereich "Status des drahtlosen Netzwerks" unter "Geschütztes drahtloses Netzwerk" auf **Aktueller Schlüssel**.

   Der für Ihr Netzwerk konfigurierte Schlüssel erscheint im Dialogfenster "Schlüsselkonfiguration".

Verwandte Themen

- Anzahl der Schlüsselrotationen einsehen (Seite 361)

Schlüssel automatisch rotieren

Standardmäßig ist die automatische Schlüsselrotation aktiviert. Wenn Sie allerdings die Schlüsselrotation aussetzen, kann diese über einen Computer mit Administratorrechten wieder aktiviert werden.

Sie können Wireless Network Security so konfigurieren, dass der Sicherheitsschlüssel eines geschützten drahtlosen Netzwerks automatisch rotiert wird.

Wireless Network Security erstellt automatisch eine unbegrenzte Serie an starken Schlüsseln, die über das Netzwerk synchronisiert wird. Die drahtlose Verbindung kann kurz unterbrochen werden, während der drahtlose Router mit der neuen Konfiguration des Sicherheitsschlüssels neu gestartet wird. Dies geschieht üblicherweise von den Netzwerkbenutzern unbemerkt.

Sollte kein Computer mit dem Netzwerk verbunden sein, tritt die Schlüsselrotation mit dem Verbindungsaufbau des ersten Computers auf.

So aktivieren Sie die automatische Schlüsselrotation:

1. Klicken Sie mit der rechten Maustaste auf das Symbol für Wireless Network Security im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Konfigurieren anzeigen** aus.
3. Markieren Sie im Bereich "Netzwerksicherheit" die Option **Automatische Schlüsselrotation aktivieren.**

   Die Schlüsselrotation kann auch vom Bereich "Status des drahtlosen Netzwerks" wieder aufgenommen werden.
4. Klicken Sie auf **Übernehmen**.

Hinweis: Die Schlüsselrotation geschieht standardmäßig alle drei Stunden. Sie können die Häufigkeit der Schlüsselrotation allerdings auf Ihre Anforderungen anpassen.

Verwandte Themen

- Schlüsselrotationshäufigkeit anpassen (Seite 346)
- Schlüsselrotation fortsetzen (Seite 346)
- Anzahl der Schlüsselrotationen einsehen (Seite 361)

Schlüsselrotation fortsetzen

Obwohl die automatische Schlüsselrotation standardmäßig aktiviert ist, kann ein Computer mit Administratorrechten die Schlüsselrotation nach einer Aussetzung wieder aufnehmen.

So nehmen Sie die Schlüsselrotation wieder auf:

1. Klicken Sie mit der rechten Maustaste auf das Symbol für Wireless Network Security im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Status anzeigen** aus.
3. Klicken Sie im Bereich "Status des drahtlosen Netzwerks" auf **Schlüsselrotation fortsetzen**.

   Die Meldungen "Schlüsselrotation gestartet" und "Sicherheitsschlüssel rotiert" bestätigen den Start der Schlüsselrotation und die erfolgreiche Durchführung.

Verwandte Themen

- Schlüssel automatisch rotieren (Seite 345)
- Automatische Schlüsselrotation aussetzen (Seite 348)
- Anzahl der Schlüsselrotationen einsehen (Seite 361)

Schlüsselrotationshäufigkeit anpassen

Wenn Wireless Network Security für die automatische Rotation des Sicherheitsschlüssels des drahtlosen Netzwerks konfiguriert ist, können Sie den Zeitraum anpassen, nach dem diese Schlüsselrotation stattfindet. Dieser Zeitraum kann von 15 Minuten bis 15 Tagen reichen.

McAfee empfiehlt eine tägliche Rotation des Sicherheitsschlüssels.

So passen Sie die automatische Schlüsselrotationshäufigkeit an:

1. Klicken Sie mit der rechten Maustaste auf das Symbol für Wireless Network Security im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Konfigurieren anzeigen** aus.
3. Bestätigen Sie im Bereich "Netzwerksicherheit", dass die automatische Schlüsselrotation aktiviert ist, und bewegen Sie den Schieberegler für die **Häufigkeit** auf eine der folgenden Positionen:
   - **alle 15 Minuten**
   - **alle 30 Minuten**
   - **jede Stunde**
   - **alle 3 Stunden**

- **alle 12 Stunden**
- **jeden Tag**
- **alle 7 Tage**
- **alle 15 Tage**

4 Klicken Sie auf **Übernehmen**.

Hinweis: Stellen Sie sicher, dass die automatische Schlüsselrotation aktiviert ist, bevor Sie die Schlüsselrotationshäufigkeit einstellen.

Verwandte Themen

- Automatische Schlüsselrotation aktivieren (Seite 345)
- Anzahl der Schlüsselrotationen einsehen (Seite 361)

Automatische Schlüsselrotation aussetzen

Die Schlüsselrotation kann von jedem Computer, der mit dem drahtlosen Netzwerk verbunden ist, ausgesetzt werden. Möglicherweise möchten Sie die Schlüsselrotation aussetzen, um Folgendes durchzuführen:

- Sie möchten einem Gast, der nicht über Wireless Network Security verfügt, den Zugriff zum Netzwerk gewähren.
- Sie möchten einem Nicht-Windows-System, z. B. Macintosh, Linux oder TiVo, Zugriff gewähren. Nachdem Sie die Schlüsselrotation angehalten haben, notieren Sie den Schlüssel, und geben Sie ihn in das neue Gerät ein.
- Sie möchten eine drahtlose Verbindung ermöglichen, die nicht durch Schlüsselrotationen unterbrochen wird, um bestimmte Programme, wie z. B. Online-Spiele, durchzuführen.
- Sie sollten die Schlüsselrotation möglichst bald fortsetzen, damit das Netzwerk vor Hackern vollständig geschützt ist.

So lassen Sie den aktuellen Schlüssel anzeigen:

1. Klicken Sie mit der rechten Maustaste auf das Symbol für Wireless Network Security im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Status anzeigen** aus.
3. Klicken Sie im Bereich "Status des drahtlosen Netzwerks" unter "Geschütztes drahtloses Netzwerk" auf **Aktueller Schlüssel**. Notieren Sie den Schlüssel, der im Dialogfenster "Schlüsselkonfiguration" angegeben ist. Andere Computer, auf denen kein Wireless Network Security installiert ist, können über diesen Schlüssel eine Verbindung zum geschützten drahtlosen Netzwerk aufbauen.
4. Klicken Sie im Dialogfenster "Schlüsselkonfiguration" auf **Schlüsselrotation aussetzen**.
5. Klicken Sie im Dialogfenster "Schlüsselrotation ausgesetzt" auf **OK**, um mit der Arbeit fortzufahren.

Warnung: Wird die Schlüsselrotation nicht ausgesetzt, verlieren die nicht unterstützten drahtlosen Geräte, die manuell mit dem Netzwerk verbunden sind, die Verbindung, wenn der Schlüssel rotiert.

Sie können eine Windows Connect Now-Disk erstellen und dann über die Textdatei den Schlüssel auf den anderen Computer oder das andere Gerät kopieren.

Verwandte Themen

- Automatische Schlüsselrotation aktivieren (Seite 345)

- Hinzufügen von Computern mithilfe der Windows Connect Now-Technologie (Seite 321)
- Schlüsselrotation fortsetzen (Seite 346)
- Schlüssel automatisch rotieren (Seite 345)
- Anzahl der Schlüsselrotationen einsehen (Seite 361)

Netzwerkschlüssel manuell rotieren

Über Wireless Network Security können Sie einen Netzwerkschlüssel manuell rotieren, auch wenn die automatische Schlüsselrotation aktiviert ist.

So rotieren Sie einen Netzwerkschlüssel manuell:

1. Klicken Sie mit der rechten Maustaste auf das Symbol für Wireless Network Security im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Tools anzeigen** aus.
3. Klicken Sie im Bereich "Extras" auf **Wartungstools**.
4. Klicken Sie auf der Seite "Wartungstools" unter **Sicherheitsschlüssel manuell rotieren** auf **Rotieren**.

   Die Meldung "Schlüsselrotation gestartet" erscheint und bestätigt, dass die Schlüsselrotation begonnen hat. Nach der Rotation des Sicherheitsschlüssels bestätigt die Meldung "Sicherheitsschlüssel rotiert", dass der Sicherheitsschlüssel erfolgreich rotiert wurde.

Hinweis: Um die Verwaltung der Sicherheitsschlüssel zu vereinfachen, können Sie im Bereich "Netzwerksicherheit" die automatische Schlüsselrotation aktivieren.

Sollte kein Computer mit Ihrem drahtlosen Netzwerk verbunden sein, tritt die automatische Schlüsselrotation mit dem Verbindungsaufbau des ersten Computers auf.

Verwandte Themen

- Automatische Schlüsselrotation aktivieren (Seite 345)
- Schlüsselrotationshäufigkeit anpassen (Seite 346)
- Anzahl der Schlüsselrotationen einsehen (Seite 361)

Schlüssel als Sternchen darstellen

Schlüssel werden standardmäßig als Sternchen dargestellt. Sie können Wireless Network Security allerdings auch so einrichten, dass die Schlüssel auf Netzwerken, die nicht durch Wireless Network Security geschützt sind, im Textformat angezeigt werden.

Netzwerke, die durch Wireless Network Security geschützt sind, zeigen die Schlüssel im Textformat an.

So lassen Sie Schlüssel als Sternchen darstellen:

1. Klicken Sie mit der rechten Maustaste auf das Symbol "Wireless Network Security" im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Konfigurieren anzeigen**.
3. Klicken Sie auf **Weitere Einstellungen**.
4. Entfernen Sie die Markierung für das Kontrollkästchen **Schlüssel in Klartext anzeigen**.
5. Klicken Sie auf **Übernehmen**.

Verwandte Themen

- Schlüssel in Klartext anzeigen (Seite 351)

Schlüssel in Klartext anzeigen

Schlüssel werden standardmäßig als Sternchen dargestellt. Sie können Wireless Network Security allerdings auch so einrichten, dass die Schlüssel auf Netzwerken, die nicht durch Wireless Network Security geschützt sind, im Textformat angezeigt werden.

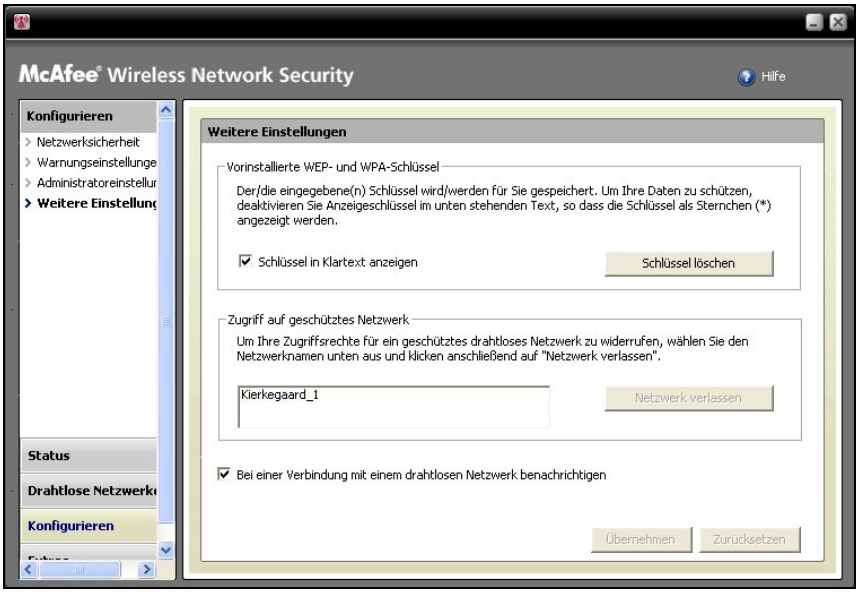
Netzwerke, die durch Wireless Network Security geschützt sind, zeigen die Schlüssel im Textformat an.

So lassen Sie Schlüssel in Klartext darstellen:

1 Klicken Sie mit der rechten Maustaste auf das Symbol "Wireless Network Security" im Windows-Benachrichtigungsbereich.

2 Wählen Sie **Konfigurieren anzeigen**.

3 Klicken Sie auf **Weitere Einstellungen**.


McAfee® Wireless Network Security
Hilfe
Konfigurieren
Netzwerksicherheit
Warnungseinstellunge
Administratoreinstellur
Weitere Einstellung
Status
Drahtlose Netzwerke
Konfigurieren
Weitere Einstellungen
Vorinstallierte WEP- und WPA-Schlüssel
Der/die eingegebene(n) Schlüssel wird/werden für Sie gespeichert. Um Ihre Daten zu schützen, deaktivieren Sie Anzeigeschlüssel im unten stehenden Text, so dass die Schlüssel als Sternchen (*) angezeigt werden.
Schlüssel in Klartext anzeigen
Schlüssel löschen
Zugriff auf geschütztes Netzwerk
Um Ihre Zugriffsrechte für ein geschütztes drahtloses Netzwerk zu widerrufen, wählen Sie den Netzwerknamen unten aus und klicken anschließend auf "Netzwerk verlassen".
Kierkegaard_1
Netzwerk verlassen
Bei einer Verbindung mit einem drahtlosen Netzwerk benachrichtigen
Übernehmen
Zurücksetzen

4 Markieren Sie das Kontrollkästchen **Schlüssel in Klartext anzeigen**.

5 Klicken Sie auf **Übernehmen**.

Verwandte Themen

- Schlüssel als Sternchen darstellen (Seite 350)

Netzwerkschlüssel löschen

Wireless Network Security speichert automatisch Ihre WEP- und vorinstallierten WPA-Schlüssel. Diese können Sie jederzeit löschen.

So löschen Sie alle Netzwerkschlüssel:

1. Klicken Sie mit der rechten Maustaste auf das Symbol "Wireless Network Security" im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Konfigurieren anzeigen**.
3. Klicken Sie im Bereich **Konfigurieren** auf **Weitere Einstellungen**.
4. Klicken Sie im Bereich **Weitere Einstellungen** unter **Vorinstallierte WEP- und WPA-Schlüssel** auf **Schlüssel löschen**.
5. Klicken Sie im Dialogfeld "Schlüssel löschen" auf **Ja**, wenn Sie sicher sind, dass Sie alle gespeicherten, vorinstallierten WEP- und WPA-Schlüssel löschen möchten.

Warnung: Durch das Löschen der Schlüssel werden diese permanent von Ihrem Computer entfernt. Nach dem Löschen der Netzwerkschlüssel müssen Sie den richtigen Schlüssel eingeben, um eine Verbindung zu einem WEP- und WPA-Netzwerk aufzubauen.

KAPITEL 44

Drahtlose Netzwerke überwachen

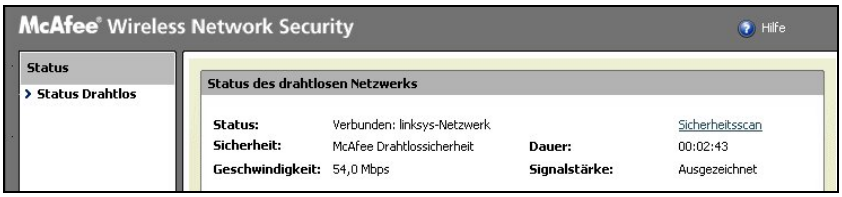
Über Wireless Network Security können Sie den Status Ihres drahtlosen Netzwerks und geschützten Computer überwachen.

In diesem Kapitel

Drahtlose Netzwerkverbindungen überwachen.....354
Geschützte drahtlose Netzwerke überwachen 360
Problembehandlung.....365

Drahtlose Netzwerkverbindungen überwachen

Im Bereich "Status des drahtlosen Netzwerks" können Sie den Status Ihrer Netzwerkverbindung, Sicherheitsmodus, Geschwindigkeit, Dauer, Signalstärke und Sicherheitsbericht ansehen.



Die folgende Tabelle beschreibt die Statusindikatoren für drahtlose Netzwerkverbindungen.

Status	Beschreibung	Informationen
Status	Zeigt an, ob Ihr Computer mit einem Netzwerk verbunden ist, und wenn ja, mit welchem.	Verbindungsstatus ansehen (Seite 355)
Sicherheit	Zeigt den Sicherheitsmodus des Netzwerks an, mit dem Sie verbunden sind. Wireless Network Security wird angezeigt, wenn Sie durch Wireless Network Security geschützt sind.	Netzwerksicherheitsmodus ansehen (Seite 357)
Geschwindigkeit	Zeigt die Geschwindigkeit der Verbindung Ihres Computers zum Netzwerk an.	Netzwerkverbindungsgeschwindigkeit ansehen (Seite 357)
Dauer	Zeigt die Zeit an, die Ihr Computer mit dem Netzwerk verbunden ist.	Dauer der Netzwerkverbindung ansehen (Seite 357)
Signalstärke	Zeigt die relative Signalstärke des Netzwerks an.	Signalstärke des Netzwerks ansehen (Seite 358)

Status	Beschreibung	Informationen
Sicherheits-scan	Durch Klicken auf **Sicherheitsscan** werden Sicherheitsinformationen, z. B. Sicherheitslücken im drahtlosen Netzwerk, Leistungsprobleme und der Status des drahtlosen Netzwerks angezeigt.	Online-Sicherheitsbericht ansehen (Seite 358)

Verwandte Themen

- Über Wireless Network Security-Symbole (Seite 324)

Verbindungsstatus ansehen

Über den Bereich "Status des drahtlosen Netzwerks" können Sie den Status der Netzwerkverbindung prüfen, um zu bestätigen, ob Sie mit dem Netzwerk verbunden sind oder nicht.

So sehen Sie den Status der drahtlosen Verbindung ein:

1. Klicken Sie mit der rechten Maustaste auf das Symbol "Wireless Network Security" im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Status anzeigen**.

   Die Computer, die mit dem geschützten Netzwerk verbunden sind, als auch Zeit und Datum der Verbindungen werden im Bereich "Status des drahtlosen Netzwerks unter **Computer** angezeigt.

Verwandte Themen

- Drahtlose Netzwerkverbindungen überwachen (Seite 354)
- Netzwerksicherheitsmodus ansehen (Seite 357)
- Netzwerkverbindungsgeschwindigkeit ansehen (Seite 357)
- Dauer der Netzwerkverbindung ansehen (Seite 357)
- Signalstärke des Netzwerks ansehen (Seite 358)
- Online-Sicherheitsbericht ansehen (Seite 358)

Netzwerksicherheitsmodus ansehen

Über den Bereich "Status der drahtlosen Verbindung" können Sie den Sicherheitsmodus der Netwerkverbindung prüfen.

So sehen Sie den Netzwerksicherheitsmodus ein:

1. Klicken Sie mit der rechten Maustaste auf das Symbol "Wireless Network Security" im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Status anzeigen**.

   Der Sicherheitsmodus wird im Bereich "Status des drahtlosen Netzwerks" im Feld **Sicherheit** angezeigt.

   Wireless Network Security wird angezeigt, wenn das drahtlose Netzwerk durch Wireless Network Security geschützt ist.

Verwandte Themen

- Drahtlose Netzwerkverbindungen überwachen (Seite 354)
- Verbindungsstatus ansehen (Seite 355)
- Netzwerkverbindungsgeschwindigkeit ansehen (Seite 357)
- Dauer der Netzwerkverbindung ansehen (Seite 357)
- Signalstärke des Netzwerks ansehen (Seite 358)
- Online-Sicherheitsbericht ansehen (Seite 358)

Netzwerkverbindungsgeschwindigkeit ansehen

Über den Bereich "Status des drahtlosen Netzwerks" können Sie die Geschwindigkeit der Verbindung Ihres Computers zum Netzwerk prüfen.

So sehen Sie die Netzwerkverbindungsgeschwindigkeit ein:

1. Klicken Sie mit der rechten Maustaste auf das Symbol "Wireless Network Security" im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Status anzeigen**.

   Die Verbindungsgeschwindigkeit wird im Bereich "Status des drahtlosen Netzwerks" im Feld **Geschwindigkeit** angezeigt.

Verwandte Themen

- Drahtlose Netzwerkverbindungen überwachen (Seite 354)
- Verbindungsstatus ansehen (Seite 355)
- Netzwerksicherheitsmodus ansehen (Seite 357)
- Dauer der Netzwerkverbindung ansehen (Seite 357)
- Signalstärke des Netzwerks ansehen (Seite 358)
- Online-Sicherheitsbericht ansehen (Seite 358)

Dauer der Netzwerkverbindung ansehen

Über den Bereich "Status des drahtlosen Netzwerks" können Sie die Dauer der Verbindung zum Netzwerk prüfen.

So sehen Sie die Dauer der Verbindung zum Netzwerk ein:

1. Klicken Sie mit der rechten Maustaste auf das Symbol "Wireless Network Security" im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Status anzeigen**.

   Die Zeitdauer, in der Ihr Computer mit dem drahtlosen Netzwerk verbunden war, wird im Feld **Dauer** angezeigt.

Verwandte Themen

- Drahtlose Netzwerkverbindungen überwachen (Seite 354)
- Verbindungsstatus ansehen (Seite 355)
- Netzwerksicherheitsmodus ansehen (Seite 357)
- Netzwerkverbindungsgeschwindigkeit ansehen (Seite 357)
- Signalstärke des Netzwerks ansehen (Seite 358)
- Online-Sicherheitsbericht ansehen (Seite 358)

Signalstärke des Netzwerks ansehen

Über den Bereich "Status der drahtlosen Verbindung" können Sie die Signalstärke des Netzwerks prüfen.

So sehen Sie die Signalstärke ein:

1. Klicken Sie mit der rechten Maustaste auf das Symbol "Wireless Network Security" im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Status anzeigen**.

   Die Qualität des Signals wird im Feld **Signalstärke** angezeigt.

Verwandte Themen

- Drahtlose Netzwerkverbindungen überwachen (Seite 354)
- Verbindungsstatus ansehen (Seite 355)
- Netzwerksicherheitsmodus ansehen (Seite 357)
- Netzwerkverbindungsgeschwindigkeit ansehen (Seite 357)
- Dauer der Netzwerkverbindung ansehen (Seite 357)
- Online-Sicherheitsbericht ansehen (Seite 358)

Online-Sicherheitsbericht ansehen

Über den Bereich "Status des drahtlosen Netzwerks" können Sie einen Bericht über Ihre drahtlose Verbindung einsehen, egal ob diese sicher oder unsicher ist.

Die McAfee Wi-FiScan-Webseite zeigt Informationen über Ihre Sicherheitslücken im drahtlosen Netzwerk, Leistungsprobleme, Informationen über Ihre drahtlose Verbindung und eine empfohlene Sicherheitslösung an und stellt dar, ob Ihre Verbindung sicher ist.

Stellen Sie vor dem Einsehen des Sicherheitsberichts sicher, dass eine Verbindung zum Internet besteht.

So sehen Sie einen Online-Sicherheitsbericht über Ihr Netzwerk ein:

1. Klicken Sie mit der rechten Maustaste auf das Symbol "Wireless Network Security" im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Status anzeigen**.
3. Klicken Sie im Bereich "Status des drahtlosen Netzwerks" auf **Sicherheitsscan**.

   Nach dem Öffnen des Browsers müssen Sie eine ActiveX-Komponente herunterladen und installieren. Abhängig von den Einstellungen des Browsers kann es möglich sein, dass Ihr Browser das Steuerelement sperrt. Erlauben Sie Ihrem Browser das Herunterladen der

Komponente und führen Sie diese aus, um den Scan durchzuführen. In Abhängigkeit von der Geschwindigkeit Ihrer Internetverbindung kann der Scan einige Zeit dauern.

Hinweis: Weitere Informationen über das Herunterladen von ActiveX-Komponenten erhalten Sie in der Dokumentation Ihres Browsers.

McAfee Wi-FiScan unterstützt Internet Explorer 5.5 und höher.

Verwandte Themen

- Drahtlose Netzwerkverbindungen überwachen (Seite 354)
- Verbindungsstatus ansehen (Seite 355)
- Netzwerksicherheitsmodus ansehen (Seite 357)
- Netzwerkverbindungsgeschwindigkeit ansehen (Seite 357)
- Dauer der Netzwerkverbindung ansehen (Seite 357)
- Signalstärke des Netzwerks ansehen (Seite 358)

Geschützte drahtlose Netzwerke überwachen

Über Wireless Network Security können Sie im Bereich "Status des drahtlosen Netzwerks" die Anzahl der Verbindungen, Schlüsselrotationen und geschützten Computer einsehen. Weiterhin können Sie Netzwerkereignisse, den aktuellen Schlüssel und derzeit geschützte Computer einsehen.

Die folgende Tabelle beschreibt die Statusindikatoren für geschützte drahtlose Netzwerkverbindungen.

Status	Beschreibung	Informationen
Schlüsselrotationen heute	Zeigt die tägliche Anzahl der Schlüsselrotationen auf dem geschützten drahtlosen Netzwerk an.	Anzahl der Schlüsselrotationen einsehen (Seite 362)
Verbindungen heute	Zeigt die tägliche Anzahl der Verbindungen zum geschützten Netzwerk an.	Anzahl der täglichen Verbindungen ansehen (Seite 362)
In diesem Monat gesicherte Computer	Zeigt die Anzahl der Computer an, die im aktuellen Monat geschützt wurden.	Anzahl der monatlich geschützten Computer ansehen (Seite 362)
Netzwerke-ereignisse	Durch Klicken auf **Netzwerkereignisse** werden Ereignisse in Bezug auf Netzwerk, Verbindung und Schlüsselrotation angezeigt.	Geschützte drahtlose Netzwerkereignisse ansehen (Seite 363)

Status	Beschreibung	Informationen
Computer	Zeigt die Anzahl der Computer an, die mit dem geschützten drahtlosen Netzwerk verbunden sind, und wann die Verbindungen aufgehoben wurden.	Derzeit geschützte Computer ansehen (Seite 364)

Anzahl der Schlüsselrotationen einsehen

Über Wireless Network Security können Sie die tägliche Anzahl der Schlüsselrotationen ansehen, die auf Ihrem geschützten Netzwerk aufgetreten sind, und wann die letzte Schlüsselrotation durchgeführt wurde.

So sehen Sie die tägliche Anzahl Schlüsselrotationen ein:

1. Klicken Sie mit der rechten Maustaste auf das Symbol "Wireless Network Security" im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Status anzeigen**.

   Im Bereich "Status des drahtlosen Netzwerks" unter **Geschütztes drahtloses Netzwerk** im Feld **Schlüsselrotationen heute** werden die Gesamtanzahl der Verbindungen und die letzte Schlüsselrotation angezeigt.

Verwandte Themen

- Geschützte drahtlose Netzwerke überwachen (Seite 360)
- Anzahl der täglichen Verbindungen ansehen (Seite 362)
- Anzahl der monatlich geschützten Computer ansehen (Seite 362)
- Geschützte drahtlose Netzwerkereignisse ansehen (Seite 363)
- Derzeit geschützte Computer ansehen (Seite 364)
- Netzwerkschlüssel verwalten (Seite 343)
- Schlüssel automatisch rotieren (Seite 345)
- Netzwerkschlüssel manuell rotieren (Seite 349)

Anzahl der täglichen Verbindungen ansehen

Über Wireless Network Security können Sie die tägliche Anzahl der Verbindungen zum geschützten Netzwerk ansehen.

So sehen Sie die Verbindungen zum geschützten drahtlosen Netzwerk ein:

1. Klicken Sie mit der rechten Maustaste auf das Symbol "Wireless Network Security" im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Status anzeigen**.

   Im Bereich "Status des drahtlosen Netzwerks" unter **Geschütztes drahtloses Netzwerk** im Feld **Verbindungen heute** wird die Gesamtanzahl der Verbindungen angezeigt.

Verwandte Themen

- Geschützte drahtlose Netzwerke überwachen (Seite 360)
- Anzahl der monatlich geschützten Computer ansehen (Seite 362)
- Geschützte drahtlose Netzwerkereignisse ansehen (Seite 363)
- Derzeit geschützte Computer ansehen (Seite 364)

Anzahl der monatlich geschützten Computer ansehen

Über Wireless Network Security können Sie die Anzahl der Computer ansehen, die im aktuellen Monat geschützt sind.

So sehen Sie die Anzahl der Computer an, die im aktuellen Monat geschützt sind:

1. Klicken Sie mit der rechten Maustaste auf das Symbol "Wireless Network Security" im Windows-Benachrichtigungsbereich.
2. Wählen Sie **Status anzeigen**.
3. Im Bereich "Status des drahtlosen Netzwerks" unter **Geschütztes drahtloses Netzwerk** im Feld **In diesem Monat gesicherte Computer** wird die Anzahl der Computer angezeigt, die im aktuellen Monat geschützt sind.

Verwandte Themen

- Geschützte drahtlose Netzwerke überwachen (Seite 360)
- Anzahl der Schlüsselrotationen einsehen (Seite 362)
- Anzahl der täglichen Verbindungen ansehen (Seite 362)
- Geschützte drahtlose Netzwerkereignisse ansehen (Seite 363)
- Derzeit geschützte Computer ansehen (Seite 364)

Geschützte drahtlose Netzwerkereignisse ansehen

Wireless Network Security protokolliert Ereignisse auf dem drahtlosen Netzwerk; z. B. wenn Sicherheitsschlüssel rotiert werden, wenn andere Computer eine Verbindung zum McAfee-geschützten Netzwerk aufbauen und wenn sich andere Computer am McAfee-geschützten Netzwerk anmelden.

Über Wireless Network Security können Sie einen Bericht einsehen, der die Ereignisse beschreibt, die auf Ihrem Netzwerk eingetreten sind. Sie können die Arten der Ereignisse festlegen, die angezeigt werden sollen und Ereignisinformationen nach Datum, Ereignis oder Computer sortieren.

So sehen Sie Netzwerkereignisse an:

1 Klicken Sie mit der rechten Maustaste auf das Symbol für Wireless Network Security im Windows-Benachrichtigungsbereich.

2 Führen Sie einen der folgenden Vorgänge aus:

Ziel	Aktion
Netzwerke- reignisse vom Bereich "Status des drahtlosen Netzwerks" aus ansehen	1. Wählen Sie **Status anzeigen** aus. 2. Klicken Sie im Bereich "Status des drahtlosen Netzwerks" unter **Geschütztes drahtloses Netzwerk** auf **Netzwerkereignisse**.
Netzwerke- reignisse vom Bereich "Status des drahtlosen Netzwerks" aus ansehen	1. Klicken Sie auf **Tools anzeigen**. 2. Klicken Sie im Bereich "Extras" auf **Wartungstools**. 3. Klicken Sie im Bereich "Wartungstools" unter **Ereignisprotokoll anzeigen** auf **Anzeigen**.

3 Wählen Sie ein oder mehrere der folgenden Ereignisse zur Anzeige aus:

- **Netzwerkereignisse**: Zeigt Informationen über Netzwerkaktivitäten an; beispielsweise den Schutz eines drahtlosen Routers oder Zugriffspunkts.

- **Verbindungsereignisse**: Zeigt Informationen über Netzwerkverbindungen an; beispielsweise Datum und Zeit, zu denen ein Computer eine Verbindung zum Netzwerk aufgebaut hat.
- **Schlüsselrotationsereignisse**: Zeigt Informationen über die Daten und Zeiten der Sicherheitsschlüsselrotationen an.

4 Klicken Sie auf **Schließen**.

Verwandte Themen

- Geschützte drahtlose Netzwerke überwachen (Seite 360)
- Anzahl der Schlüsselrotationen einsehen (Seite 362)
- Anzahl der täglichen Verbindungen ansehen (Seite 362)
- Anzahl der täglichen Verbindungen ansehen (Seite 362)
- Derzeit geschützte Computer ansehen (Seite 364)

Derzeit geschützte Computer ansehen

Sie können die Anzahl der Computer ansehen, die mit dem geschützten drahtlosen Netzwerk verbunden sind, und wann jeweils deren letzte Verbindung stattfand.

So sehen Sie die Computer ein, die eine Verbindung zum geschützten Netzwerk aufgebaut haben:

1 Klicken Sie mit der rechten Maustaste auf das Symbol "Wireless Network Security" im Windows-Benachrichtigungsbereich.

2 Wählen Sie **Status anzeigen**.

3 Die Computer, die mit dem geschützten Netzwerk verbunden sind, als auch Zeit und Datum der jeweils letzten Verbindung werden im Bereich "Status des drahtlosen Netzwerks" unter **Computer** angezeigt.

Verwandte Themen

- Geschützte drahtlose Netzwerke überwachen (Seite 360)
- Anzahl der Schlüsselrotationen einsehen (Seite 362)
- Anzahl der täglichen Verbindungen ansehen (Seite 362)
- Anzahl der monatlich geschützten Computer ansehen (Seite 362)
- Geschützte drahtlose Netzwerkereignisse ansehen (Seite 363)

KAPITEL 45

Problembehandlung

Wenn Sie Wireless Network Security und Geräte von Fremdanbietern verwenden, können Sie Fehlerbehebungen vornehmen. Zu den behebbaren Problemen gehören:

- Installationsschwierigkeiten
- Schutz oder Konfiguration Ihres Netzwerks ist nicht möglich
- Verbindungsaufbau von Computern zum Netzwerk nicht möglich
- Verbindungsaufbau zu einem Netzwerk oder zum Internet nicht möglich
- Andere Probleme

In diesem Kapitel

Installieren von Wireless Network Security.....366
Schützen oder Konfigurieren des Netzwerks 368
Verbinden von Computern mit Ihrem Netzwerk.....371
Verbindung zum Internet und Netzwerk aufbauen .373
Andere Probleme.....379

Installieren von Wireless Network Security

Sie können die folgenden Installationsprobleme beheben:

- Auf welchen Computern muss diese Software installiert werden?
- Drahtloser Adapter wird nicht erkannt
- Mehrere drahtlose Adapter
- Kein Download auf drahtlose Computer möglich, da das Netzwerk bereits sicher ist

Auf welchen Computern muss diese Software installiert werden?

Installieren Sie Wireless Network Security auf allen drahtlosen Computern im Netzwerk (im Gegensatz zu anderen McAfee-Programmen können Sie diese Software auf mehreren Computern installieren). Befolgen Sie die Lizenzvereinbarung der erworbenen Software. In einigen Fällen kann es notwendig sein, zusätzliche Lizenzen zu erwerben.

Auf Computern ohne drahtlosen Adapter können Sie die Software installieren (müssen dies aber nicht tun). Auf diesen Computern ist die Software nicht aktiv, weil sie keinen entsprechenden Schutz benötigen.

Wireless Network Security wird derzeit von Windows XP oder Windows 2000 unterstützt.

Kompatibler drahtloser Adapter wird nicht erkannt

Wenn der drahtlose Adapter nach dem Installieren und Aktivieren nicht erkannt wird, müssen Sie den Computer neu starten. Wird der Adapter anschließend immer noch nicht erkannt, sollten Sie folgendermaßen vorgehen:

1. Öffnen Sie das Windows-Dialogfeld "Eigenschaften von Drahtlose Netzwerkverbindungen".
2. Klicken Sie unter Verwendung des klassischen Startmenüs von Windows auf **Start**, zeigen Sie auf **Einstellungen**, und wählen Sie **Netzwerkverbindungen** aus.
3. Klicken Sie auf das Symbol **Drahtlose Netzwerkverbindung**.
4. Klicken Sie im Dialogfeld "Status der drahtlosen Netzwerkverbindung" auf **Eigenschaften**.
5. Entfernen Sie im Bereich "Eigenschaften der drahtlosen Netzwerkverbindung" die Markierung für **MWL-Filter**, und nehmen Sie die Markierung erneut vor.

6. Klicken Sie auf **OK**.

   Sollte dieser Vorgang das Problem nicht behoben haben, führen Sie eine Prüfung mithilfe von Wi-FiScan durch. Wenn Wi-FiScan funktioniert, wird Ihr Adapter unterstützt. Wenn nicht, müssen Sie Ihren Adaptertreiber aktualisieren (über Windows-Aktualisierung, oder besuchen Sie die Webseite des Herstellers) oder einen neuen Treiber erwerben.

Verwandte Themen

- Online-Sicherheitsbericht ansehen (Seite 358)

Mehrere drahtlose Adapter

Wenn in einer Fehlermeldung steht, dass mehrere drahtlose Adapter installiert sind, müssen Sie alle bis auf einen deaktivieren oder vom Netzwerk trennen. Wireless Network Security funktioniert nur mit einem drahtlosen Adapter.

Download schlägt auf sicherem Netzwerk fehl

Installieren Sie, falls Sie über eine CD verfügen, Wireless Network Security von der CD auf allen drahtlosen Computern.

Wenn Sie die Software auf einem drahtlosen Computer installiert und das Netzwerk geschützt haben, bevor Sie die Software auf allen anderen Computern installiert haben, verfügen Sie über folgende Optionen.

- Heben Sie den Schutz des Netzwerks auf. Laden Sie dann die Software herunter, und installieren Sie sie auf allen drahtlosen Computern. Schützen Sie Ihr Netzwerk wieder.
- Zeigen Sie den Netzwerkschlüssel an. Geben Sie dann den Schlüssel auf Ihrem drahtlosen Computer ein, um eine Verbindung zum Netzwerk herzustellen. Laden Sie die Software herunter, installieren Sie diese, und melden Sie sich vom drahtlosen Computer aus am Netzwerk an.
- Laden Sie die ausführbare Datei auf den Computer herunter, der bereits mit dem Netzwerk verbunden ist, und speichern Sie diese auf einem USB-Flash-Laufwerk, oder brennen Sie sie auf eine CD, damit Sie sie auf den anderen Computern installieren können.
- Führen Sie die Windows Connect Now-Technologie aus.

Verwandte Themen

- Drahtlose Router oder Zugriffspunkte entfernen (Seite 333)
- Aktuelle Schlüssel anzeigen (Seite 344)
- Hinzufügen von Computern über Wechselgeräte (Seite 319)
- Hinzufügen von Computern mithilfe der Windows Connect Now-Technologie (Seite 321)

Schützen oder Konfigurieren des Netzwerks

Sie können die folgenden Probleme in Bezug auf den Schutz und die Konfiguration Ihres Netzwerks beheben:

- Nicht unterstützter Router oder Zugriffspunkt
- Aktualisieren der Firmware des Routers oder Zugriffspunkts
- Fehler durch doppelte Administratoren
- Netzwerk als ungesichert angezeigt
- Keine Reparatur möglich

Nicht unterstützter Router oder Zugriffspunkt

Wenn es in einer Fehlermeldung heißt, dass der drahtlose Router oder Zugriffspunkt unter Umständen nicht unterstützt wird, konnte das Gerät von Wireless Network Security nicht konfiguriert werden, weil es nicht erkannt oder gefunden wurde.

Stellen Sie durch Anforderung eines Updates sicher, dass Sie über die neueste Version von Wireless Network Security verfügen (McAfee weitet die Unterstützung ständig auf neue Router und Zugriffspunkte aus). Wenn der Router oder Zugriffspunkt in der Liste der unterstützten Router aufgeführt wird und dieser Fehler dennoch auftritt, liegen Kommunikationsprobleme zwischen Ihrem Computer und dem Router oder Zugriffspunkt vor.

Verwandte Themen

- Unterstützte drahtlose Router
  http://www.mcafee.com/router

Aktualisieren der Firmware des Routers oder Zugriffspunkts

Wenn es in einer Fehlermeldung heißt, dass die Firmware-Version des drahtlosen Routers oder Zugriffspunkts nicht unterstützt wird, wird zwar das Gerät unterstützt, nicht aber dessen Firmware-Version. Stellen Sie durch Anforderung eines Updates sicher, dass Sie über die neueste Version von Wireless Network Security verfügen (McAfee weitet die Unterstützung ständig auf neue Firmware-Versionen aus).

Wenn Sie über die neueste Version von Wireless Network Security verfügen, sollten Sie die Website des Herstellers des Routers oder Zugriffspunkts aufrufen bzw. sich an dessen Support wenden und eine in der Liste unterstützter Router aufgelistete Firmware-Version installieren.

Verwandte Themen

- Unterstützte drahtlose Router
  http://www.mcafee.com/router

Fehler durch doppelte Administratoren

Nach dem Konfigurieren des Routers oder Zugriffspunkts müssen Sie sich von der Administrationsoberfläche abmelden. Geschieht das nicht, verhält der Router oder Zugriffspunkt sich in einigen Fällen so, als würde er weiterhin von einem anderen Computer konfiguriert werden. Es wird dann eine Fehlermeldung angezeigt.

Wenn Sie sich nicht abmelden können, ziehen Sie das Stromkabel Ihres Routers oder Zugriffspunkts heraus, und stecken Sie es dann wieder ein.

Fehler bei der Schlüsselrotation

Fehlerursache:

- Die Anmeldeinformationen für Ihren Router oder Zugriffspunkt wurden geändert.
- Die Firmware-Version Ihres Routers oder Zugriffspunkts wurde geändert, und die neue Version wird nicht unterstützt.
- Ihr Router oder Zugriffspunkt ist nicht verfügbar. Stellen Sie sicher, dass der Router oder Zugriffspunkt eingeschaltet und an das Netzwerk angeschlossen ist.
- Fehler durch doppelte Administratoren.
- Bei einigen drahtlosen Routern kann es vorkommen, dass der McAfee-Client nicht in der Lage ist, auf das Management Interface zuzugreifen, um den Verschlüsselungsschlüssel zu rotieren, wenn bereits ein anderer Computer auf der Weboberfläche des drahtlosen Routers manuell angemeldet ist.

Verwandte Themen

- Informationen für drahtlose Geräte ändern (Seite 341)
- Schlüssel automatisch rotieren (Seite 345)

Reparieren des Routers oder Zugriffspunkts nicht möglich

Gehen Sie folgendermaßen vor, wenn bei der Reparatur Fehler auftreten. Beachten Sie, dass die einzelnen Verfahren voneinander unabhängig sind.

- Stellen Sie per Kabel eine Verbindung zu Ihrem Netzwerk her, und wiederholen Sie dann den Reparaturvorgang.
- Ziehen Sie das Stromkabel des Routers oder Zugriffspunkts, und stecken Sie es dann wieder ein. Versuchen Sie dann, eine Verbindung herzustellen.
- Setzen Sie den drahtlosen Router oder Zugriffspunkt auf die Werkseinstellungen zurück, und reparieren Sie ihn. Hierdurch werden die drahtlosen Einstellungen auf die Standardeinstellungen zurückgesetzt. Setzen Sie dann die Einstellungen für Ihre Internetverbindung zurück.
- Verlassen Sie mithilfe der erweiterten Optionen das Netzwerk auf allen Computern, setzen Sie den drahtlosen Router oder Zugriffspunkt auf die Werkseinstellungen zurück, und schützen Sie ihn dann. Hierdurch werden die drahtlosen Einstellungen auf die Standardeinstellungen zurückgesetzt. Setzen Sie dann die Einstellungen für Ihre Internetverbindung zurück.

Verwandte Themen

- Netzwerk-Sicherheitseinstellungen reparieren (Seite 342)

Netzwerk scheint ungeschützt

Wenn das Netzwerk als ungesichert angezeigt wird, ist es nicht geschützt. Sie müssen das Netzwerk schützen. Beachten Sie, dass Wireless Network Security ausschließlich mit kompatiblen Routern und Zugriffspunkten funktionsfähig ist.

Verwandte Themen

- Geschützte drahtlose Netzwerke erstellen (Seite 308)
- Unterstützte drahtlose Router
  http://www.mcafee.com/router

Verbinden von Computern mit Ihrem Netzwerk

Sie können die folgenden Probleme in Bezug auf die Verbindung von Computern zum Netzwerk beheben:

- Warten auf Autorisierung
- Gewähren von Zugriff für einen unbekannten Computer

Warten auf Autorisierung

Wenn Sie sich an einem geschützten Netzwerk anzumelden versuchen und der Computer vergeblich auf Autorisierung wartet, sollten Sie Folgendes überprüfen.

- Ein drahtloser Computer mit bestehendem Zugriff auf das Netzwerk ist eingeschaltet und mit dem Netzwerk verbunden.
- An diesem Computer ist jemand anwesend, der Zugriff erteilen kann, wenn Ihr Computer angezeigt wird.
- Die Computer befinden sich innerhalb der Reichweite der Funkwellen.

Wenn **Zugriff gewähren** auf dem Computer mit bestehendem Zugriff auf das Netzwerk nicht angezeigt wird, müssen Sie versuchen, den Zugriff von einem anderen Computer aus zu gewähren.

Falls keine anderen Computer verfügbar sind, müssen Sie den Schutz des Netzwerks vom Computer mit vorhandenem Zugriff aus aufheben und das Netzwerk vom Computer ohne Zugriff aus schützen. Melden Sie sich anschließend von dem Computer aus am Netzwerk an, der das Netzwerk ursprünglich schützte.

Weiterhin können Sie die Funktion "Anderen Computer schützen" verwenden.

Verwandte Themen

- Anmelden an einem geschützten drahtlosen Netzwerk (Seite 310)
- Geschützte drahtlose Netzwerke verlassen (Seite 336)
- Drahtlose Router oder Zugriffspunkte entfernen (Seite 333)
- Computer zum geschützten drahtlosen Netzwerk hinzufügen (Seite 319)

Gewähren von Zugriff für einen unbekannten Computer

Wenn Sie von einem unbekannten Computer eine Anfrage auf die Gewährung von Zugriff erhalten, sollten Sie diese ablehnen, bis dessen Legitimität bestätigt ist. Möglicherweise versucht ein Unbefugter, auf Ihr Netzwerk zuzugreifen.

Verbindung zum Internet und Netzwerk aufbauen

Sie können die folgenden Probleme in Bezug auf die Verbindung zu einem Netzwerk oder zum Internet beheben:

- Schlechte Verbindung zum Internet
- Kurze Unterbrechung der Verbindung
- Verbindungsverlust bei Geräten (nicht beim Computer)
- Aufforderung zur Eingabe des WEP-, WPA- oder WPA2-Schlüssels
- Keine Verbindung möglich
- Aktualisieren des drahtlosen Adapters
- Schwaches Signal
- Windows kann die drahtlose Verbindung nicht konfigurieren
- Windows zeigt keine Verbindung an

Verbindung zum Internet kann nicht hergestellt werden

Wenn Sie keine Verbindung herstellen können, schließen Sie den Computer mit einem Kabel an das Netzwerk an, und stellen Sie dann eine Verbindung zum Internet her. Ist immer noch keine Verbindung möglich, sollten Sie die folgenden Punkte überprüfen:

- Ihr Modem ist eingeschaltet
- Ihre PPPoE-Einstellungen sind korrekt
- Ihre DSL- oder Kabelleitung ist aktiv

Verbindungsprobleme, etwa mit der Geschwindigkeit und der Signalstärke, können auch durch Funkstörungen verursacht werden. Versuchen Sie das Problem über die folgenden Methoden zu beheben:

- Ändern Sie den Kanal des schnurlosen Telefons.
- Beseitigen Sie mögliche Störquellen.
- Ändern Sie den Standort des drahtlosen Routers, Zugriffspunkts oder Computers.
- Ändern Sie den Kanal von Router oder Zugriffspunkt. Die Kanäle 1, 4, 7 und 11 werden für Nord- und Südamerika empfohlen. Die Kanäle 1, 4, 7, 13 werden für die anderen Länder empfohlen. Viele Router sind standardmäßig auf Kanal 6 eingestellt.
- Stellen Sie sicher, dass weder Router noch drahtloser Adapter (insbesondere ein drahtloser USB-Adapter) nicht gegen eine Wand eingerichtet sind.
- Stellen Sie sicher, dass sich Ihr drahtloser USB-Adapter nicht neben einem drahtlosen AP/Router befindet.
- Stellen Sie den Router entfernt von Wänden und metallischen Gegenständen auf.

Verbindung unterbrochen

Wenn Ihre Verbindung kurzzeitig unterbrochen wird (z. B. während eines Online-Spiels), kann eine Schlüsselrotation die Ursache hierfür sein. Um dies zu verhindern, können Sie die Schlüsselrotation aussetzen.

Sie sollten die Schlüsselrotation möglichst bald fortsetzen, damit das Netzwerk vor Hackern vollständig geschützt ist.

Verwandte Themen

- Schlüssel automatisch rotieren (Seite 345)
- Schlüsselrotation fortsetzen (Seite 346)
- Automatische Schlüsselrotation aussetzen (Seite 348)
- Netzwerkschlüssel manuell rotieren (Seite 349)

Verbindungsverlust bei Geräten

Wenn einige Geräte die Verbindung verlieren, während Wireless Network Security eingesetzt wird, versuchen Sie das Problem durch eine der folgenden Methoden zu beheben:

- Setzen Sie die Schlüsselrotation aus
- Aktualisieren Sie den Treiber für den drahtlosen Adapter
- Deaktivieren Sie den Client-Manager des Adapters

Verwandte Themen

- Automatische Schlüsselrotation aussetzen (Seite 348)

Aufforderung zur Eingabe des WEP-, WPA- oder WPA2-Schlüssels

Wenn Sie zum Herstellen einer Verbindung zum geschützten drahtlosen Netzwerk einen WEP-, WPA- oder WPA2-Schlüssel eingeben müssen, haben Sie wahrscheinlich die Software nicht auf Ihrem Computer installiert.

Für eine ordnungsgemäße Funktionsweise muss Wireless Network Security auf allen drahtlosen Computern im Netzwerk installiert sein.

Verwandte Themen

- Wireless Network Security starten (Seite 302)
- Computer zum geschützten drahtlosen Netzwerk hinzufügen (Seite 319)

Verbindung zum drahtlosen Netzwerk nicht möglich

Wenn Sie keine Verbindung herstellen können, gehen Sie folgendermaßen vor: Beachten Sie, dass die einzelnen Verfahren voneinander unabhängig sind.

- Vergewissern Sie sich, falls Sie keine Verbindung zu einem geschützten Netzwerk herstellen, dass Sie über den richtigen Schlüssel verfügen. Geben Sie ihn erneut ein.
- Ziehen Sie den Stecker des drahtlosen Adapters, und stecken Sie ihn wieder ein. Oder deaktivieren Sie den Adapter, und aktivieren Sie ihn dann wieder.
- Schalten Sie den Router oder Zugriffspunkt aus und wieder ein. Versuchen Sie dann, eine Verbindung herzustellen.
- Vergewissern Sie sich, dass der drahtlose Router oder Zugriffspunkt verbunden ist, und reparieren Sie die Sicherheitseinstellungen.
- Starten Sie den Computer neu.
- Aktualisieren Sie den drahtlosen Adapter, oder erwerben Sie einen neuen. Beispiel: Ihr Netzwerk setzt WPA-PSK

TKIP-Sicherheit ein, und Ihr drahtloser Adapter unterstützt den Sicherheitsmodus des Netzwerks nicht (die Netzwerke zeigen WEP an, obwohl sie auf WPA festgelegt sind).

- Wenn Sie nach dem Aktualisieren des drahtlosen Routers oder Zugriffspunkts keine Verbindung herstellen können, haben Sie möglicherweise auf eine nicht unterstützte Version aktualisiert. Vergewissern Sie sich, dass der Router oder Zugriffspunkt unterstützt wird. Wenn dies nicht der Fall ist, sollten Sie eine unterstützte Version installieren oder warten, bis ein Update von Wireless Network Security verfügbar ist.

Verwandte Themen

- Netzwerk-Sicherheitseinstellungen reparieren (Seite 342)
- Aktualisieren des drahtlosen Adapters (Seite 376)

Aktualisieren des drahtlosen Adapters

Eventuell müssen Sie Ihren drahtlosen Adapter aktualisieren, um Wireless Network Security verwenden zu können.

So aktualisieren Sie Ihren Adapter:

1. Klicken Sie auf dem Desktop auf **Start**, zeigen Sie auf **Einstellungen**, und wählen Sie dann **Systemsteuerung** aus.
2. Doppelklicken Sie auf das Symbol **System**. Das Dialogfeld **Systemeigenschaften** wird angezeigt.
3. Wählen Sie die Registerkarte **Hardware** aus, und klicken Sie dann auf **Geräte-Manager**.
4. Doppelklicken Sie in der Liste **Geräte-Manager** auf Ihren Adapter.
5. Wählen Sie die Registerkarte **Treiber** aus, und notieren Sie sich den Treiber, der bei Ihnen installiert ist.
6. Besuchen Sie die Webseite des Adapterherstellers, um nach einer Aktualisierung zu suchen. Treiber sind meist im Support- oder Download-Bereich zu finden. Wenn Sie eine Mini-PCI-Karte verwenden, gehen Sie zur Webseite des Herstellers des Computers und nicht des Kartenherstellers.
7. Wenn ein Treiber-Update verfügbar ist, folgen Sie den Anweisungen auf der Website, um das Update herunterzuladen.
8. Gehen Sie zurück zur Registerkarte **Treiber**, und klicken Sie auf **Aktualisieren**. Ein Windows-Assistent wird angezeigt.
9. Befolgen Sie die Anweisungen auf der Webseite, um den Treiber zu installieren.

Schwaches Signal

Wenn Ihre Verbindung unterbrochen wird oder sehr langsam ist, ist möglicherweise das Signal zu schwach. Gehen Sie wie folgt vor, um das Signal zu verbessern:

- Stellen Sie sicher, dass die drahtlosen Geräte nicht durch Metallobjekte wie Öfen, Rohre oder große Haushaltsgeräte blockiert werden. Funksignale werden stark abgeschwächt, wenn sie durch solche Objekte hindurch verlaufen.
- Wenn das Signal durch Wände gelangen muss, sollten Sie sicherstellen, dass dies nicht im spitzen Winkel geschieht. Je länger der Weg innerhalb der Wand ist, desto schwächer wird das Signal.
- Verfügt der drahtlose Router oder Zugriffspunkt über zwei Antennen, sollten Sie die beiden Antennen nach Möglichkeit rechtwinklig zueinander ausrichten (eine vertikal und eine horizontal im 90-Grad-Winkel).
- Einige Hersteller verwenden Hochleistungsantennen. Richtantennen haben eine größere Reichweite, während omnidirektionale Antennen (Rundstrahler) die größte Flexibilität bieten. Richten Sie sich beim Installieren der Antenne nach den entsprechenden Anweisungen des Herstellers.

Führen diese Schritte nicht zum Erfolg, sollten Sie dem Netzwerk einen Zugriffspunkt hinzufügen, der sich näher an dem Computer befindet, zu dem Sie eine Verbindung herstellen möchten. Wenn Sie den zweiten Zugriffspunkt mit demselben Netzwerknamen (SSID) und einem anderen Kanal konfigurieren, sucht der Adapter automatisch das stärkste Signal und stellt die Verbindung über den entsprechenden Zugriffspunkt her.

Verwandte Themen

- Signalstärkensymbole (Seite 325)
- Signalstärke des Netzwerks ansehen (Seite 358)

Windows unterstützt keine drahtlose Verbindung

Wenn Sie eine Windows-Meldung darauf hinweist, dass die drahtlose Verbindung nicht konfiguriert werden kann, können Sie diese Meldung ignorieren. Verwenden Sie Wireless Network Security, um Verbindungen zu drahtlosen Netzwerken herzustellen und die Netzwerke zu konfigurieren.

Stellen Sie sicher, dass im Windows-Dialogfeld "Eigenschaften von Drahtlose Netzwerkverbindung" auf der Registerkarte "Drahtlosnetzwerke" das Kontrollkästchen **Windows zum Konfigurieren der Einstellungen verwenden** deaktiviert ist.

Wireless Network Security ermöglicht folgende Dinge:

- Adapter, die an Computern mit Windows 2000 installiert sind, können eine Verbindung zu WPA-Netzwerken aufbauen, auch wenn der Karten-Client-Manager nicht unterstützt wird.
- Adapter an Computern, auf denen Windows XP läuft, können eine Verbindung zu WPA2-Netzwerken aufbauen, ohne dass der Win XP SP2-Hotfix installiert werden muss.
- Adapter unter Windows XP SP1 können eine Verbindung zu WPA- und WPA2-Netzwerken aufbauen, ohne dass ein Hotfix installiert werden muss, der nicht von Windows XP SP1 unterstützt wird.

Windows zeigt keine Verbindung an

Wenn Sie verbunden sind, das Netzwerksymbol von Windows jedoch ein X anzeigt (d. h. keine Verbindung), so können Sie das ignorieren. Ihre Verbindung ist einwandfrei.

Andere Probleme

Sie können die folgenden Probleme beheben:

- Bei Verwendung anderer Programme lautet der Netzwerkname anders
- Probleme beim Konfigurieren drahtloser Router oder Zugriffspunkte
- Ersetzen von Computern
- Auswahl eines anderen Sicherheitsmodus
- Software funktioniert nach dem Aktualisieren des Betriebssystems nicht

Bei Verwendung anderer Programme lautet der Netzwerkname anders

Dass der Name des Netzwerks in anderen Programmen anders angezeigt wird (etwa mit _SafeAaf als Bestandteil des Namens), ist völlig normal.

Wireless Network Security kennzeichnet Netzwerke mit einem Code, wenn sie geschützt sind.

Drahtlose Router oder Zugriffspunkte konfigurieren

Wenn beim Konfigurieren des Routers oder Zugriffspunkts oder beim Hinzufügen mehrerer Router im Netzwerk ein Fehler auftritt, müssen Sie sich vergewissern, dass alle Router und Zugriffspunkte über eine eigene IP-Adresse verfügen.

Wenn der Name des drahtlosen Routers oder Zugriffspunkts im Dialogfeld "Drahtlosen Router/Zugriffspunkt schützen" aufgeführt wird, Sie jedoch bei dessen Konfiguration eine Fehlermeldung erhalten, müssen Sie überprüfen, ob der Router oder Zugriffspunkt unterstützt wird.

Wenn der Router oder Zugriffspunkt konfiguriert ist, sich aber scheinbar nicht im richtigen Netzwerk befindet (es werden zum Beispiel keine anderen Computer im LAN angezeigt), müssen Sie sicherstellen, dass Sie den richtigen Router oder Zugriffspunkt konfiguriert haben, und nicht den Ihres Nachbarn. Ziehen Sie das Stromkabel des Routers oder Zugriffspunkts, und vergewissern Sie sich, dass die Verbindung unterbrochen wird. Wenn Sie den falschen Router oder Zugriffspunkt konfiguriert haben, heben Sie dessen Schutz wieder auf, und schützen Sie dann den richtigen Router oder Zugriffspunkt.

Wenn Sie den Router oder Zugriffspunkt nicht ordnungsgemäß konfigurieren oder hinzufügen können, er aber unterstützt wird, liegt das unter Umständen daran, dass Sie Änderungen durchgeführt haben, die nun eine ordnungsgemäße Konfiguration verhindern.

- Folgen Sie den Anweisungen des Herstellers zum Konfigurieren Ihres drahtlosen Routers bzw. Zugriffspunkts für DHCP oder zum Festlegen der richtigen IP-Adresse. In einigen Fällen ist ein Konfigurations-Tool im Lieferumfang des Produkts enthalten.
- Setzen Sie den Router oder Zugriffspunkt auf die Werkseinstellungen zurück, und versuchen Sie erneut, das Netzwerk zu reparieren. Möglicherweise haben Sie den Administrationsport am Router oder Zugriffspunkt geändert oder die drahtlose Administration deaktiviert. Stellen Sie sicher, dass Sie die Standardkonfiguration verwenden und dass die drahtlose Konfiguration aktiviert ist. Eine weitere Möglichkeit besteht darin, dass die http-Administration deaktiviert ist. Stellen Sie in diesem Fall sicher, dass sie aktiviert ist. Stellen Sie sicher, dass Sie Port 80 für die Administration verwenden.
- Wenn der drahtlose Router oder Zugriffspunkt nicht in der Liste drahtloser Router oder Zugriffspunkte aufgeführt wird, die geschützt und zu denen Verbindungen hergestellt werden sollen, müssen Sie die SSID-Übertragung aktivieren und sicherstellen, dass Ihr Router oder Zugriffspunkt in der Liste der verfügbaren Netzwerke von Wireless Network Security aufgelistet ist.

- Falls Sie getrennt werden oder keine Verbindung herstellen können, ist möglicherweise die MAC-Filterung aktiviert. Deaktivieren Sie sie.
- Wenn zwischen zwei Computern mit drahtloser Verbindung zum Netzwerk keine Netzwerkvorgänge möglich sind (zum Beispiel die Freigabe von Dateien oder das Drucken auf freigegebenen Druckern), müssen Sie überprüfen, ob die Isolierung von Zugriffspunkten nicht aktiviert ist. Sie verhindert, dass drahtlose Computer über das Netzwerk miteinander in Verbindung treten können.
- Wenn Sie eine andere Firewall als die McAfee Personal Firewall verwenden, müssen Sie sicherstellen, dass das Subnet vertrauenswürdig ist.

Verwandte Themen

- Unterstützte drahtlose Router
  http://www.mcafee.com/router

Ersetzen von Computern

Wenn der Computer, der das Netzwerk geschützt hat, ersetzt wurde und es keine anderen Computer mit Zugriff gibt (d. h. Sie können nicht auf das Netzwerk zugreifen), setzen Sie den drahtlosen Router oder Zugriffspunkt auf die Werkseinstellungen zurück, und schützen Sie das Netzwerk erneut.

Auswahl eines anderen Sicherheitsmodus

Wenn eine Fehlermeldung darauf hinweist, dass Sie einen Sicherheitsmodus ausgewählt haben, der vom drahtlosen Adapter nicht unterstützt wird, müssen Sie einen anderen Sicherheitsmodus auswählen.

- Alle Adapter unterstützen WEP.
- Die meisten Adapter, die WPA unterstützen, verwenden sowohl WPA-PSK TKIP- als auch WPA-PSK AES-Sicherheitsmodi.
- Adapter, die WPA2 unterstützen, verwenden WPA-Sicherheitsmodi und WPA2-PSK TKIP, WPA2-PSK AES und WPA2-PSK TKIP/AES.

Verwandte Themen

- Konfigurieren von Sicherheitseinstellungen (Seite 338)
- Netzwerksicherheitsmodus ansehen (Seite 356)

Software funktioniert nach Aktualisierung des Betriebssystems nicht

Wenn Wireless Network Security nach der Aktualisierung von Betriebssystemen nicht funktionieren sollte, entfernen Sie das Programm, und installieren Sie es neu.

KAPITEL 46

McAfee EasyNetwork

McAfee(R) EasyNetwork ermöglicht sichere Dateifreigabe, vereinfachte Dateiübertragungen und automatische Druckerfreigabe für die Computer in Ihrem privaten Netzwerk.

Bevor Sie mit der Verwendung von EasyNetwork beginnen, sollten Sie sich mit einigen der bekanntesten Funktionen vertraut machen. Details zur Konfiguration und Verwendung dieser Funktionen finden Sie in der Hilfe zu EasyNetwork.

In diesem Kapitel

Funktionen 384
EasyNetwork einrichten 385
Dateien freigeben und senden 393
Drucker freigeben 399

Funktionen

EasyNetwork bietet folgende Funktionen:

Dateifreigabe

EasyNetwork vereinfacht die Dateifreigabe auf Ihrem Computer für andere Computer im Netzwerk. Wenn Sie Dateien freigeben, gewähren Sie anderen Computern schreibgeschützten Zugriff auf diese Dateien. Nur Computer, die Mitglied des verwalteten Netzwerks sind (d. h. vollen oder Administratorzugriff haben), können Dateien freigeben oder auf Dateien zugreifen, die von anderen Mitgliedern freigegeben wurden.

Dateiübertragung

Sie können Dateien an andere Computer senden, die Mitglied des verwalteten Netzwerks sind. Wenn Sie eine Datei empfangen, wird diese in Ihrem EasyNetwork-Eingangsbereich angezeigt. Der Eingangsbereich ist ein temporärer Speicherort für alle Dateien, die andere Computer im Netzwerk an Sie senden.

Automatisierte Druckerfreigabe

Wenn Sie Mitglied eines verwalteten Netzwerks werden, gibt EasyNetwork automatisch alle lokalen Drucker frei, die an Ihren Computer angeschlossen sind. Dabei verwendet es für den Namen der Druckerfreigabe den aktuellen Namen des Druckers. EasyNetwork erkennt zudem Drucker, die von anderen Computern in Ihrem Netzwerk freigegeben wurden, und ermöglicht Ihnen, diese Drucker zu konfigurieren und zu verwenden.

KAPITEL 47

EasyNetwork einrichten

Bevor Sie die EasyNetwork-Funktionen verwenden können, müssen Sie das Programm starten und sich beim verwalteten Netzwerk anmelden. Nach der Anmeldung können Sie das Netzwerk jederzeit wieder verlassen.

In diesem Kapitel

Starten von EasyNetwork 386
Anmelden an einem verwalteten Netzwerk 387
Verwaltetes Netzwerk verlassen.....391

Starten von EasyNetwork

Standardmäßig werden Sie direkt nach der Installation von EasyNetwork gefragt, ob Sie das Programm starten möchten; Sie können EasyNetwork jedoch auch später starten.

EasyNetwork starten

Sie werden standardmäßig aufgefordert, EasyNetwork direkt nach der Installation zu starten. Sie können es jedoch auch zu einem späteren Zeitpunkt starten.

So starten Sie EasyNetwork:

- Klicken Sie im Menü **Start** auf **Programme**, **McAfee** und anschließend auf **McAfee EasyNetwork**.

Tipp: Wenn Sie während der Installation das Erstellen von Desktop- und Schnellstartsymbolen gewählt haben, können Sie EasyNetwork auch starten, indem Sie auf dem Desktop auf das McAfee EasyNetwork-Symbol doppelklicken oder indem Sie im Benachrichtigungsbereich rechts neben der Taskleiste auf das McAfee EasyNetwork-Symbol klicken.

Anmelden an einem verwalteten Netzwerk

Nach der Installation von SecurityCenter wird Ihrem Computer ein Netzwerkagent hinzugefügt, der im Hintergrund ausgeführt wird. In EasyNetwork ist der Netzwerkagent verantwortlich für das Finden einer gültigen Netzwerkverbindung, das Finden lokaler Drucker zur Freigabe und das Überwachen des Netzwerkstatus.

Wenn in dem Netzwerk, in dem Sie sich derzeit befinden, kein anderer Computer gefunden wird, der den Netzwerkagenten ausführt, werden Sie automatisch zu einem Mitglied dieses Netzwerks gemacht und müssen angeben, ob das Netzwerk vertrauenswürdig ist. Da Ihr Computer der erste ist, der dem Netzwerk beitritt, erscheint der Name Ihres Computers als Teil des Netzwerknamens; Sie können das Netzwerk jedoch jederzeit umbenennen.

Wenn ein Computer eine Verbindung mit dem Netzwerk herstellt, wird an alle anderen Computer, die sich bereits im Netzwerk verbinden, eine Beitrittsanfrage gesendet. Diese Anfrage kann von jedem Computer genehmigt werden, der über administrative Berechtigung für das Netzwerk verfügt. Der Computer, der Zugriff gewährt, kann die Berechtigungsstufe für den Computer festlegen, der gerade dem Netzwerk beitritt; beispielsweise Gast (nur Dateiübertragung) oder vollständig/administrativ (Dateiübertragung und Dateifreigabe). In EasyNetwork können Computer mit administrativem Zugriff anderen Computern Zugriff gewähren und Berechtigungen verwalten (d. h. Computer mit mehr oder weniger Rechten versehen); Computer mit vollständigem Zugriff können diese administrativen Aufgaben nicht ausführen. Bevor der Computer dem Netzwerk beitreten darf, wird außerdem eine Sicherheitsüberprüfung durchgeführt.

Hinweis: Wenn Sie andere Netzwerkprogramme von McAfee installiert haben (z. B. McAfee Wireless Network Security oder Network Manager), wird der Computer nach dem Beitritt auch in diesen Programmen als verwalteter Computer erkannt. Die Berechtigungsstufe, die einem Computer zugewiesen wird, gilt für alle McAfee-Netzwerkprogramme. Weitere Informationen dazu, was Gastberechtigungen, vollständige oder administrative Berechtigungen in anderen McAfee-Netzwerkprogrammen bedeuten, finden Sie in der Dokumentation zu dem jeweiligen Programm.

Dem Netzwerk beitreten

Wenn ein Computer zum ersten Mal nach der Installation von EasyNetwork einem vertrauenswürdigen Netzwerk beitritt, wird der Benutzer gefragt, ob er dem verwalteten Netzwerk beitreten möchte. Wenn der Benutzer des Computers dem Beitritt zustimmt, wird an alle anderen Computer im Netzwerk, die über administrativen Zugriff verfügen, eine Anfrage gesendet. Diese Anfrage muss genehmigt werden, bevor der Computer Drucker oder Dateien freigeben oder Dateien im Netzwerk senden oder kopieren kann. Wenn der Computer der erste Computer im Netzwerk ist, werden ihm automatisch administrative Genehmigungen verliehen.

So treten Sie dem Netzwerk bei:

1. Klicken Sie im Fenster "Freigegebene Dateien" auf **Ja, diesem Netzwerk jetzt beitreten**.
   Wenn ein administrativer Computer im Netzwerk Ihre Anfrage genehmigt, wird eine Nachricht angezeigt, in der festgelegt werden muss, ob dieser Computer und andere Computer im Netzwerk die Sicherheitseinstellungen der jeweils anderen Computer verwalten dürfen.
2. Wen dieser Computer und andere Computer im Netzwerk die Sicherheitseinstellungen der jeweils anderen Computer verwalten sollen, klicken Sie auf **Ja**; klicken Sie andernfalls auf **Nein**.
3. Bestätigen Sie, dass der Computer, der den Netzwerkzugriff gewährt, die Spielkarten anzeigt, die derzeit im Dialogfeld für die Bestätigung der Sicherheit angezeigt werden, und klicken Sie auf **Bestätigen**.

Hinweis: Wenn der Computer, der Ihnen den Zugriff gewährt hat, nicht dieselben Spielkarten anzeigt, die auch im Dialogfeld für die Sicherheitsbestätigung angezeigt werden, liegt im verwalteten Netzwerk ein Sicherheitsverstoß vor. Durch das Anmelden am Netzwerk ist Ihr Computer möglicherweise einem Risiko ausgesetzt. Klicken Sie deshalb im Dialogfeld für die Bestätigung der Sicherheit auf **Ablehnen**.

Zugriff auf das Netzwerk gewähren

Wenn ein Computer dem verwalteten Netzwerk beitreten möchte, wird den anderen Computern im Netzwerk, die über administrativen Zugriff verfügen, eine Nachricht gesendet. Der erste Computer, der auf diese Nachricht antwortet, ist der Computer, der Zugriff gewährt. Der Computer, der Zugriff gewährt, entscheidet, welche Art von Zugriff dem Computer gewährt wird: Gast, vollständig oder administrativ

So gewähren Sie Zugriff auf das Netzwerk:

1. Aktivieren Sie in der Nachricht eines der folgenden Kontrollkästchen:
   - **Zugriff als Gast gewähren**: Der Benutzer kann Dateien an andere Computer senden, aber keine Dateien freigeben.
   - **Vollständigen Zugriff auf alle verwalteten Netzwerkanwendungen gewähren**: Der Benutzer kann Dateien senden und freigeben.
   - **Administrativen Zugriff auf alle verwalteten Netzwerkanwendungen gewähren**: Der Benutzer kann Dateien senden und freigeben, anderen Computern Zugriff gewähren und die Berechtigungsstufen anderer Computer anpassen.
2. Klicken Sie auf **Zugriff gewähren**.
3. Bestätigen Sie, dass der Computer die Spielkarten anzeigt, die derzeit im Dialogfeld für die Bestätigung der Sicherheit angezeigt werden, und klicken Sie auf **Bestätigen**.

Hinweis: Wenn der Computer nicht dieselben Spielkarten anzeigt, die auch im Dialogfeld für die Sicherheitsbestätigung angezeigt werden, liegt im verwalteten Netzwerk ein Sicherheitsverstoß vor. Durch das Gewähren des Zugriffs für diesen Computer ist Ihr Computer möglicherweise einem Risiko ausgesetzt. Klicken Sie deshalb im Dialogfeld für die Bestätigung der Sicherheit auf **Ablehnen**.

Netzwerk umbenennen

Standardmäßig beinhaltet der Netzwerkname den Namen des ersten Computers, der dem Netzwerk beigetreten ist; Sie können den Netzwerknamen jedoch jederzeit ändern. Wenn Sie den Netzwerknamen ändern, können Sie die Netzwerkbeschreibung ändern, die in EasyNetwork angezeigt wird.

So benennen Sie das Netzwerk um:

1. Klicken Sie im Menü **Optionen** auf **Konfiguration**.
2. Geben Sie im Dialogfeld "Konfiguration" den Namen des Netzwerks in das Feld **Netzwerkname** ein.
3. Klicken Sie auf **OK**.

Verwaltetes Netzwerk verlassen

Wenn Sie sich bei einem verwalteten Netzwerk anmelden und anschließend entscheiden, dass Sie nicht länger Mitglied dieses Netzwerks sein möchten, können Sie das Netzwerk verlassen. Wenn Sie Ihre Mitgliedschaft aufgegeben haben, können Sie sich jederzeit wieder anmelden. Ihnen muss jedoch die Berechtigung zum Anmelden gewährt und die Sicherheitsprüfung muss erneut ausgeführt werden. Weitere Informationen finden Sie unter Bei einem verwalteten Netzwerk anmelden (Seite 387).

Verwaltetes Netzwerk verlassen

Sie können ein verwaltetes Netzwerk verlassen, bei dem Sie sich zuvor angemeldet haben.

So verlassen Sie ein verwaltetes Netzwerk:

1. Klicken Sie im Menü **Tools** auf **Netzwerk verlassen**.
2. Wählen Sie im Dialogfeld "Netzwerk verlassen" den Namen des Netzwerks, das Sie verlassen möchten.
3. Klicken Sie auf **Netzwerk verlassen**.

KAPITEL 48

Dateien freigeben und senden

EasyNetwork vereinfacht das Freigeben und Senden von Dateien auf Ihrem Computer für andere Computer im Netzwerk. Wenn Sie Dateien freigeben, gewähren Sie anderen Computern schreibgeschützten Zugriff auf diese Dateien. Nur Computer, die Mitglied des verwalteten Netzwerks sind (d. h. vollen oder Administratorzugriff haben), können Dateien freigeben oder auf Dateien zugreifen, die von anderen Mitgliedern freigegeben wurden.

In diesem Kapitel

Dateien freigeben.....394
Senden von Dateien an andere Computer.....397

Dateien freigeben

EasyNetwork vereinfacht die Dateifreigabe auf Ihrem Computer für andere Computer im Netzwerk. Wenn Sie Dateien freigeben, gewähren Sie anderen Computern schreibgeschützten Zugriff auf diese Dateien. Nur Computer, die Mitglied des verwalteten Netzwerks sind (d. h. vollen oder Administratorzugriff haben), können Dateien freigeben oder auf Dateien zugreifen, die von anderen Mitgliedern freigegeben wurden. Wenn Sie einen Ordner freigeben, werden alle darin und in den Unterordnern enthaltenen Dateien freigegeben. Nachträglich hinzugefügte Dateien werden jedoch nicht automatisch freigegeben. Wenn eine freigegebene Datei oder ein freigegebener Ordner gelöscht wird, wird sie bzw. er automatisch aus dem Fenster "Freigegebene Dateien" entfernt. Sie können eine Dateifreigabe jederzeit rückgängig machen.

Sie haben zwei Möglichkeiten, auf eine freigegebene Datei zuzugreifen: indem Sie die Datei direkt in EasyNetwork öffnen oder sie auf Ihren Computer kopieren und sie dann öffnen. Wenn Ihre Liste der Dateifreigaben zu lang ist, können Sie nach der freigegebenen Datei suchen, auf die Sie zugreifen möchten.

Hinweis: Auf Dateien, die über EasyNetwork freigegeben wurden, kann von anderen Computern mit Windows-Explorer nicht zugegriffen werden. Das Freigeben von Dateien über EasyNetwork erfolgt über sichere Verbindungen.

Freigabe einer Datei

Wenn Sie eine Datei freigeben, können automatisch alle anderen Mitglieder mit vollständigem oder administrativem Zugriff auf das verwaltete Netzwerk darauf zugreifen.

So geben Sie eine Datei frei:

1. Finden Sie in Windows-Explorer die Datei, die Sie freigeben möchten.
2. Ziehen Sie die Datei von ihrem Speicherort in Windows-Explorer auf das Fenster "Freigegebene Dateien" in EasyNetwork.

Tipp: Sie können eine Datei auch freigeben, indem Sie auf **Dateien freigeben** im Menü **Extras** klicken. Navigieren Sie im Dialogfeld "Freigeben" zu dem Ordner, in dem sich die Datei befindet, die freigegeben werden soll, wählen Sie die Datei aus, und klicken Sie auf **Freigeben**.

Freigabe einer Datei aufheben

Wenn Sie eine Datei im verwalteten Netzwerk freigeben, können Sie diese Freigabe jederzeit aufheben. Wenn Sie die Freigabe einer Datei aufheben, können andere Mitglieder des verwalteten Netzwerks nicht mehr darauf zugreifen.

So heben Sie die Freigabe einer Datei auf:

1. Klicken Sie im Menü **Extras** auf **Freigabe von Dateien stoppen**.
2. Wählen Sie im Dialogfeld "Freigabe von Dateien stoppen" die Datei aus, die Sie nicht mehr freigeben möchten.
3. Klicken Sie auf **Nicht freigeben**.

Freigegebene Datei kopieren

Sie können freigegebene Dateien von einem beliebigen Computer im verwalteten Netzwerk auf Ihren Computer kopieren. Wenn der Computer die Dateifreigabe anschließend stoppt, verfügen Sie noch über eine Kopie der Datei.

So kopieren Sie eine Datei:

- Ziehen Sie die Datei aus dem Fenster "Freigegebene Dateien" in EasyNetwork an einen Speicherort in Windows-Explorer oder auf dem Windows-Desktop.

Tipp: Sie können eine freigegebene Datei auch kopieren, indem Sie die Datei in EasyNetwork auswählen und anschließend im Menü **Tools** auf **Kopie an** klicken. Navigieren Sie im Dialogfeld "Kopieren in Ordner" zu dem Ordner, in den Sie die Datei kopieren möchten, wählen Sie die Datei aus und klicken Sie anschließend auf **Speichern**.

Suchen nach einer freigegebenen Datei

Sie können nach einer Datei suchen, die von Ihnen oder einem anderen Mitglied des Netzwerks freigegeben wurde. Während der Eingabe der Suchkriterien zeigt EasyNetwork automatisch die entsprechenden Ergebnisse im Fenster "Freigegebene Dateien" an.

So suchen Sie nach einer freigegebenen Datei:

1. Klicken Sie im Fenster "Freigegebene Dateien" auf **Suche**.
2. Klicken Sie in der Liste **Enthält** auf eine der folgenden Optionen:
   - **Alle Begriffe**: Sucht nach Datei- oder Pfadnamen, die alle Wörter enthalten, die Sie in der Liste **Datei oder Pfadnamen** angeben, in beliebiger Reihenfolge.

- **Ein beliebiger Begriff**: Sucht nach Datei- oder Pfadnamen, die eines der Wörter enthalten, die Sie in der Liste **Datei oder Pfadnamen** angeben.
- **Exakte Zeichenfolge**: Sucht nach Datei- oder Pfadnamen, die den exakten Ausdruck enthalten, den Sie in der Liste **Datei oder Pfadnamen** angeben.

3 Geben Sie einen Teil oder den gesamten Datei- oder Pfadnamen in die Liste **Datei oder Pfadname** ein.

4 Klicken Sie in der Liste **Typ** auf einen der folgenden Dateitypen:

- **Beliebig**: Durchsucht alle freigegebenen Dateitypen.
- **Dokument**: Durchsucht alle freigegebenen Dokumente.
- **Bild**: Durchsucht alle freigegebenen Bilddateien.
- **Video**: Durchsucht alle freigegebenen Videodateien.
- **Audio**: Durchsucht alle freigegebenen Audiodateien.

5 Klicken Sie in den Listen **Von** und **Bis** auf die Daten, die den Datumsbereich festlegen, in dem die Datei erstellt wurde.

Senden von Dateien an andere Computer

Sie können Dateien an andere Computer senden, die Mitglieder des verwalteten Netzwerks sind. Vor dem Senden einer Datei überprüft EasyNetwork, ob der Computer, der die Datei enthält, über ausreichend freien Speicherplatz verfügt.

Wenn Sie eine Datei erhalten, wird diese in Ihrem EasyNetwork-Posteingang angezeigt. Der Posteingang ist ein temporärer Speicherort für alle Dateien, die Sie von anderen Computern im Netzwerk erhalten. Wenn EasyNetwork geöffnet ist, wenn Sie eine Datei erhalten, wird die Datei sofort in Ihrem Posteingang angezeigt; andernfalls wird eine Nachricht im Benachrichtigungsbereich rechts der Windows-Taskleiste angezeigt. Wenn Sie keine Benachrichtigungen erhalten möchten, können Sie diese deaktivieren. Wenn eine Datei mit demselben Namen bereits im Posteingang vorhanden ist, wird dem Namen der neuen Datei eine Zahl als Suffix hinzugefügt. Dateien bleiben in Ihrem Posteingang, bis Sie sie akzeptieren (sie also an einen Speicherort auf Ihrem Computer kopieren).

Eine Datei an einen anderen Computer senden

Sie können eine Datei direkt an einen anderen Computer im verwalteten Netzwerk senden, ohne sie freizugeben. Bevor ein Benutzer die Datei auf dem empfangenden Computer anzeigen kann, muss sie lokal gespeichert werden. Weitere Informationen hierzu finden Sie unter Dateien von einem anderen Computer akzeptieren (Seite 398).

So senden Sie eine Datei an einen anderen Computer:

1. Suchen Sie die zu sendende Datei in Windows-Explorer.
2. Ziehen Sie die Datei in Windows-Explorer von ihrem Speicherort auf ein aktives Computersymbol in EasyNetwork.

Tipp: Sie können mehrere Dateien an einen Computer senden, indem Sie beim Auswählen der Dateien die STRG-Taste gedrückt halten. Sie können die Dateien auch senden, indem Sie im Menü **Tools** auf **Senden** klicken, die Dateien auswählen und anschließend auf **Senden** klicken.

Akzeptieren einer Datei von einem anderen Computer

Wenn ein anderer Computer im verwalteten Netzwerk Ihnen eine Datei sendet, müssen Sie diese akzeptieren (indem Sie sie in einem Ordner auf Ihrem Computer speichern). Wenn EasyNetwork nicht geöffnet ist oder sich nicht im Vordergrund befindet, wenn eine Datei an Ihren Computer gesendet wird, erhalten Sie eine Benachrichtigung im Benachrichtigungsbereich rechts der Taskleiste. Klicken Sie auf die Benachrichtigung, um EasyNetwork zu öffnen und auf die Datei zuzugreifen.

So erhalten Sie eine Datei von einem anderen Computer:

- Klicken Sie auf **Erhalten** und ziehen Sie eine Datei von Ihrem EasyNetwork-Posteingang in einen Ordner in Windows-Explorer.

Tipp: Sie können eine Datei von einem anderen Computer auch erhalten, indem Sie die Datei in Ihrem EasyNetwork-Posteingang auswählen und im Menü **Extras** auf **Akzeptieren** klicken. Navigieren Sie im Dialogfeld "Akzeptieren für Ordner" auf den Ordner, in dem die Dateien, die Sie erhalten, gespeichert werden sollen, wählen Sie ihn aus, und klicken Sie auf **Speichern**.

Benachrichtigung bei gesendeter Datei erhalten

Sie können eine Benachrichtigung erhalten, wenn ein anderer Computer im verwalteten Netzwerk Ihnen eine Datei sendet. Wenn EasyNetwork aktuell nicht geöffnet oder auf dem Desktop nicht im Vordergrund angezeigt wird, wird rechts neben der Windows-Taskleiste eine Benachrichtigungsmeldung angezeigt.

So erhalten Sie Benachrichtungen bei gesendeten Dateien:

1. Kllicken Sie im Menü **Optionen** auf **Konfigurieren**.
2. Aktivieren Sie im Dialogfeld "Konfigurieren" das Kontrollkästchen **Benachrichtigen, wenn Dateien von anderen Computern gesendet werden**.
3. Klicken Sie auf **OK**.

KAPITEL 49

Drucker freigeben

Wenn Sie sich bei einem verwalteten Netzwerk angemeldet haben, gibt EasyNetwork automatisch alle mit Ihrem Computer verbundenen lokalen Drucker frei. EasyNetwork erkennt zudem Drucker, die von anderen Computern in Ihrem Netzwerk freigegeben wurden, und ermöglicht Ihnen, diese Drucker zu konfigurieren und zu verwenden.

In diesem Kapitel

Mit freigegebenen Druckern arbeiten 400

Mit freigegebenen Druckern arbeiten

Wenn Sie Mitglied eines verwalteten Netzwerks werden, gibt EasyNetwork automatisch alle lokalen Drucker frei, die an Ihren Computer angeschlossen sind. Dabei verwendet es für den Namen der Druckerfreigabe den aktuellen Namen des Druckers. EasyNetwork erkennt zudem Drucker, die von anderen Computern in Ihrem Netzwerk freigegeben wurden, und ermöglicht Ihnen, diese Drucker zu konfigurieren und zu verwenden. Wenn Sie einen Druckertreiber über einen Netzwerk-Druckerserver konfiguriert haben (z. B. ein Wireless-USB-Druckerserver), betrachtet EasyNetwork den Drucker als lokalen Drucker und gibt ihn automatisch im Netzwerk frei. Sie können eine Druckerfreigabe jederzeit rückgängig machen.

EasyNetwork erkennt auch Drucker, die von allen anderen Computern im Netzwerk freigegeben wurden. Wenn es einen Remote-Drucker erkennt, der noch nicht mit Ihrem Computer verbunden ist, wird beim erstmaligen Öffnen von EasyNetwork im Fenster "Freigegebene Dateien" der Link **Verfügbare Netzwerkdrucker** angezeigt. Dies ermöglicht Ihnen, verfügbare Drucker zu installieren oder Drucker zu deinstallieren, die mit Ihrem Computer bereits verbunden sind. Sie können zudem die Liste der im Netzwerk erkannten Drucker aktualisieren.

Wenn Sie sich beim verwalteten Netzwerk noch nicht angemeldet haben, mit diesem aber bereits verbunden sind, können Sie über die Drucker-Systemsteuerung von Windows auf die freigegebenen Drucker zugreifen.

Freigabe eines Druckers aufheben

Sie können die Freigabe eines Druckers jederzeit aufheben. Mitglieder, die den Drucker installiert haben, können ihn nicht mehr zum Drucken verwenden.

So heben Sie die Freigabe eines Druckers auf:

1. Klicken Sie im Menü **Extras** auf **Drucker**.
2. Klicken Sie im Dialogfeld "Netzwerkdrucker verwalten" auf den Namen des Druckers, den Sie nicht mehr freigeben möchten.
3. Klicken Sie auf **Nicht freigeben**.

Installieren eines verfügbaren Netzwerkdruckers

Als Mitglied eines verwalteten Netzwerks können Sie auf die Drucker zugreifen, die im Netzwerk freigegeben sind. Dazu müssen Sie die Druckertreiber installieren, die der Drucker verwendet. Wenn der Eigentümer des Druckers dessen Freigabe aufhebt, nachdem Sie ihn installiert haben, können Sie mit diesem Drucker nicht mehr drucken.

So installieren Sie einen verfügbaren Netzwerkdrucker:

1. Klicken Sie im Menü **Extras** auf **Drucker**.
2. Klicken Sie im Dialogfeld "Verfügbare Netzwerkdrucker" auf den Namen eines Druckers.
3. Klicken Sie auf **Installieren**.

KAPITEL 50

Referenz

Das Begriffsglossar enthält und definiert die am häufigsten in McAfee-Produkten verwendete Sicherheitsterminologie.

Info zu McAfee enthält rechtliche Informationen zu McAfee Corporation.

Glossar

"

"Man-in-the-Middle"-Angriff

Der Angreifer fängt Nachrichten bei einem öffentlichen Schlüsselaustausch ab und überträgt sie neu, wobei er den angeforderten Schlüssel durch deren eigene öffentliche Schlüssel ersetzt, so dass die beiden ursprünglichen Parteien weiterhin den Eindruck haben, direkt miteinander zu kommunizieren. Dabei verwendet der Angreifer ein Programm, dass sich dem Client gegenüber als Server und dem Server gegenüber als Client ausgibt. Der Angriff kann dazu dienen, einfach nur Zugriff auf die Nachrichten zu erhalten. Der Angreifer hat aber auch die Möglichkeit, die Nachrichten zu ändern, bevor er sie wieder weiterleitet. Der Begriff leitet sich von einem Ballspiel ab, bei dem mehrere Personen versuchen, sich gegenseitig den Ball zuzuwerfen, während ein einzelner Mitspieler in der Mitte versucht, den Ball abzufangen.

8

802.11

Eine Reihe von IEEE-Standards für Funk-LANs. 802.11 legt eine Schnittstelle für den Funkverkehr zwischen einem drahtlosen Client und einer Basisstation oder zwischen zwei drahtlosen Clients fest. Zu den verschiedenen Spezifikationen von 802.11 gehören die Standards 802.11a (für Netzwerke mit einer Bandbreite bis zu 54 Mbit/s im 5 GHz-Band), 802.11b (für Netzwerke mit einer Bandbreite bis zu 11 Mbit/s im 2,4 GHz-Band), 802.11g (für Netzwerke mit einer Bandbreite bis zu 54 Mbit/s im 2,4 GHz-Band) sowie 802.11i (eine Reihe von Sicherheitsstandards für alle drahtlosen Ethernet-Netzwerke).

802.11a

Eine Erweiterung von 802.11 für Funk-LANs zum Senden von Daten mit einer Bandbreite bis zu 54 Mbit/s im 5 GHz-Band. Dabei ist die Übertragungsgeschwindigkeit zwar größer als bei 802.11b, die Reichweite ist jedoch viel geringer.

802.11b

Eine Erweiterung von 802.11 für Funk-LANs, die eine Bandbreite von 11 Mbit/s im 2,4 GHz-Band bietet. 802.11b gilt derzeit als Standard für drahtlose Netzwerkverbindungen.

802.11g

Eine Erweiterung von 802.11 für Funk-LANs, die eine Bandbreite von 54 Mbit/s im 2,4 GHz-Band bietet.

802.1x

Wird von Wireless Home Network Security nicht unterstützt. Ein IEEE-Standard für die Authentifizierung in kabelgebundenen und drahtlosen Netzwerken, wird aber vor allem in Verbindung mit drahtlosen 802.11-Netzwerken verwendet. Dieser Standard bietet eine starke gegenseitige Authentifizierung zwischen einem Client und einem Authentifizierungsserver. Außerdem bietet 802.1x dynamische, benutzer- und sitzungsspezifische WEP-Schlüssel, wodurch der bei statischen WEP-Schlüsseln übliche Verwaltungsaufwand und die Sicherheitsrisiken beseitigt werden.

A

Anschluss

Hierbei handelt es sich um einen Ort, an dem Informationen bei einem Computer ein- oder ausgehen. Ein konventionelles Analogmodem ist beispielsweise an einen seriellen Anschluss angeschlossen. Die Anschlussnummern bei der TCP/IP-Kommunikation sind virtuelle Werte, die den Datenverkehr in anwendungsspezifische Datenströme aufteilen. Anschlüsse werden Standardprotokollen wie SMTP oder HTTP zugeordnet, damit die Programme "wissen", über welchen Anschluss eine Verbindung hergestellt werden kann. Der Zielanschluss für TCP-Pakete gibt die gesuchte Anwendung oder den gesuchten Server an.

archivieren

Mithilfe dieser Optionen können Sie eine Kopie Ihrer überwachten Dateien lokal auf einem CD-, DVD- oder USB-Laufwerk, einer externen Festplatte oder einem Netzwerk-Laufwerk erstellen.

archivieren

Mithilfe dieser Optionen können Sie eine Kopie Ihrer überwachten Dateien lokal auf einem CD-, DVD- oder USB-Laufwerk, einer externen Festplatte oder einem Netzwerk-Laufwerk erstellen.

Authentifizierung

Der Vorgang des Identifizierens eines bestimmten Benutzers, meist anhand von Benutzername und Kennwort. Mit der Authentifizierung wird sichergestellt, dass es sich bei einem Benutzer auch wirklich um denjenigen handelt, der er oder sie zu sein vorgibt. Über die Zugriffsrechte dieses Benutzers sagt die Authentifizierung jedoch nichts aus.

B

Bandbreite

Die Datenmenge, die innerhalb eines bestimmten Zeitraums übertragen werden kann. Bei digitalen Geräten wird die Bandbreite meist in Bit pro Sekunde (Bit/s) oder Byte pro Sekunde angegeben. Bei analogen Geräten wird die Bandbreite als Taktzahl pro Sekunde bzw. Hertz (Hz) angegeben.

Bibliothek

Der Online-Speicherbereich für Dateien, die von Benutzern der Datensicherung veröffentlicht werden. Die Bibliothekt ist eine Website im Internet, auf die jeder mit Internetzugriff zugreifen kann.

Bilderanalyse

Verhindert die Anzeige potentiell unangemessener Bilder. Bilder werden für alle Benutzer blockiert, außer für Mitglieder der Altersgruppe "Erwachsener".

Browser

Ein Clientprogramm, das mit Hilfe von HTTP (Hypertext Transfer Protocol) Anforderungen an Webserver im Internet richtet. Ein Webbrowser zeigt dem Benutzer den Inhalt graphisch an.

Brute-Force-Angriff

Eine Vorgehensweise nach dem Fehler-Treffer-Prinzip, die auch unter dem Begriff "Brute-Force-Cracking" bekannt ist. Dabei versuchen entsprechende Programme, verschlüsselte Daten (z. B. Kennwörter) mithilfe eines riesigen Aufwands (mit "purer Gewalt") anstatt durch zielgerichtete Strategien zu entschlüsseln.
Brute-Force-Anwendungen probieren nacheinander alle möglichen Kombinationen von zulässigen Zeichen aus – wie bei einem Safe, bei dem alle Zahlenkombinationen ausprobiert werden, um ihn zu öffnen, was genauso eine strafbare Handlung ist.
Brute-Force-Angriffe werden als eine Methode betrachtet, die, wenn auch mit großen Zeitaufwand verbunden, irgendwann schließlich zum Erfolg führt.

C

chiffrierter Text

Das sind Daten, die verschlüsselt wurden. Chiffrierter Text ist nicht lesbar, solange er nicht mithilfe eines Schlüssels wieder in Klartext umgewandelt (entschlüsselt) wurde.

Client

Eine Anwendung, die auf einem PC oder einer Workstation ausgeführt wird und zum Durchführen bestimmter Vorgänge auf einen Server angewiesen ist. Beispiel: Ein E-Mail-Client ist eine Anwendung, mit der Sie E-Mails senden und empfangen können.

Cookie

Ein Datenblock im World Wide Web, den ein Webserver auf einem Clientsystem speichert. Wenn ein Benutzer erneut dieselbe Website besucht, sendet der Browser eine Kopie des Cookies zurück an den Server. Cookies werden für die Identifizierung von Benutzern, zur Anweisung an den Server, eine benutzerdefinierte Version der angeforderten Webseite zu senden, zum Senden von Kontoinformationen an den Benutzer sowie für andere administrative Aufgaben verwendet.

Diese Datei ermöglicht es, dass die Website sich an Sie "erinnert", und der Betreiber kann feststellen, wie viele Benutzer die Website besucht haben bzw. wann welche Seiten der Website aufgerufen wurden. Unternehmen versuchen, ihre Websites mithilfe von Cookies gezielt auf die Vorlieben und Anforderungen verschiedener Benutzer abzustimmen. Zahlreiche Websites gestatten beispielsweise den Zugriff auf bestimmte Seiten der Website erst dann, wenn Sie einen Benutzernamen und ein Kennwort eingeben, und senden ein Cookie an Ihren Computer, so dass Sie sich beim nächsten Besuch dieser Seiten nicht erneut anmelden müssen. Cookies können jedoch auch missbraucht werden. Online-Werbefirmen verwenden oft Cookies, um zu analysieren, welche Websites häufig von Ihnen besucht werden, und nutzen diese Erkenntnisse zum Platzieren von Werbeanzeigen auf den meistbesuchten Websites. Bevor Sie Cookies von einer Website zulassen, sollten Sie sicher sein, dass Sie dieser Website vertrauen können.

Cookies sind nicht nur für rechtsgültige Unternehmen eine Informationsquelle, sondern können zu diesem Zweck auch von Hackern missbraucht werden. Zahlreiche Websites von Onlineshops speichern Kreditkartennummern und andere persönliche Informationen in Cookies, um den Kunden das Einkaufen zu erleichtern. Leider sind Sicherheitslücken nicht auszuschließen, die es Hackern ermöglichen, über die auf den Kundencomputern gespeicherten Cookies auf vertrauliche Daten zuzugreifen.

D

Denial of Service, DoS

Ein DoS-Angriff (Denial-of-Service, Dienstverweigerung) ist ein Störfall im Internet, durch den Benutzer oder Unternehmen nicht mehr auf bestimmte Ressourcen oder Dienste zugreifen können. Dabei handelt es sich meist um die Nichtverfügbarkeit eines einzelnen Netzwerkdienstes (z. B. E-Mail) oder den vorübergehenden Verlust aller Netzwerkverbindungen und -dienste. Im schlimmsten Fall kann beispielsweise eine Website, auf die täglich Millionen Benutzer zugreifen, zeitweise gezwungen sein, ihren Betrieb einzustellen. Bei einem DoS-Angriff können auch Programme und Dateien in einem Computersystem zerstört werden. Auch wenn DoS-Angriffe meist absichtlich und böswillig sind, können sie manchmal auch unbeabsichtigt passieren. Ein DoS-Angriff stellt eine Art von Sicherheitsverletzung dar, die meist nicht zu einem Diebstahl von Informationen oder anderen Sicherheitsverlusten führt. Trotzdem können solche Angriffe für die Zielperson bzw. das geschädigte Unternehmen mit einem beträchtlichen Zeitaufwand und erheblichen Kosten verbunden sein.

DNS

Acronym für Domain Name System. Das hierarchische System, über das Hosts im Internet sowohl Domänennamenadressen (wie bluestem.prairienet.org) und IP-Adressen (wie 192.17.3.4) erhalten. Die Domänennamenadresse wird von Personen verwendet und automatisch in die numerische IP-Adresse übersetzt, die von der Paket-Weiterleitungssoftware verwendet wird. DNS-Namen bestehen aus einer Domäne auf der obersten Ebene (wie .com, .org, und .net), einer Domäne auf der zweiten Ebene (der Site-Name eines Unternehmens, einer Organisation oder einer Einzelperson) und möglicherweise einer oder mehreren untergeordneten Domänen (Server innerhalb einer Domäne auf der zweiten Ebene). Siehe auch DNS-Server und IP-Adresse.

DNS-Server

Abkürzung für Domain Name System-Server. Ein Computer, der Domain Name System (DNS)-Abfragen beantworten kann. Der DNS-Server verwaltet eine Datenbank mit Host-Computern und ihren dazugehörigen IP-Adressen. Der DNS-Server, der durch den Namen apex.com dargestellt wird, würde beispielsweise die IP-Adresse des fiktiven Unternehmens Apex zurückgeben. Auch bezeichnet als: Namensserver Siehe auch DNS- und IP-Adresse.

Domäne

Eine Adresse einer Netzwerkverbindung, die den Inhaber dieser Adresse in einem hierarchischen Format identifiziert: server.organisation.typ. Beispielsweise bezeichnet www.whitehouse.gov den Webserver des Weißen Hauses, das Teil der US-Regierung ist.

Drahtloser Adapter

Enthält die Schaltkreise, mit denen ein Computer oder ein anderes Gerät mit einem (an einem drahtlosen Netzwerk angeschlossenen) drahtlosen Router kommunizieren kann. Drahtlose Adapter können entweder im Hauptschaltkreis eines Hardwaregeräts integriert sein oder sich auf einer separaten Zusatzkarte befinden, die in den entsprechenden Anschluss eines Geräts eingesteckt wird.

E

E-Mail

E-Mails sind "elektronische Post", also Nachrichten, die über das Internet oder innerhalb eines Unternehmens über LAN oder WAN gesendet werden. E-Mail-Anlagen in Form von EXE-Dateien (ausführbare Dateien) oder VBS-Dateien (Visual Basic-Skriptdateien) werden immer häufiger für die Übertragung von Viren und trojanischen Pferden zweckentfremdet.

E-Mail-Client

Ein E-Mail-Konto. Beispielsweise Microsoft Outlook oder Eudora.

Echtzeit-Scans

Dateien werden auf Viren und andere Aktivitäten gescannt, wenn Sie oder Ihr Computer darauf zugreifen.

Ereignis

Ereignisse von 0.0.0.0

Wenn Ereignisse mit der IP-Adresse 0.0.0.0 angezeigt werden, gibt es hierfür zwei mögliche Ursachen. Die erste und häufigste Ursache ist die, dass Ihr Computer ein fehlerhaftes Paket erhalten hat. Das Internet ist nicht zu 100 % zuverlässig, und es ist immer möglich, dass fehlerhafte Pakete eingehen. Da Firewall die Pakete vor der TCP/IP-Validierung erhält, kann es solche Pakete möglicherweise als Ereignis melden.

Die zweite Ursache ist die, dass die Quell-IP-Adresse gefälscht wurde. Gefälschte Pakete sind möglicherweise ein Anzeichen dafür, dass jemand auf Ihrem Computer nach einem Trojaner gesucht hat. Vergessen Sie nicht, dass Firewall diesen Versuch blockiert.

Ereignisse von 127.0.0.1

Manchmal wird von Ereignissen als IP-Quelladresse 127.0.0.1 angegeben. Hierbei ist zu beachten, dass es sich um eine spezielle IP-Adresse handelt, die auch Loopbackadresse genannt wird.

Unabhängig davon, welchen Computer Sie verwenden, 127.0.0.1 bezieht sich stets auf Ihren lokalen Computer. Diese Adresse wird auch Localhost genannt, weil der Computername "Localhost" immer die IP-Adresse 127.0.0.1 auflöst. Bedeutet dies, dass der Computer einen Angriff auf sich selbst ausübt? Wird Ihr Computer von einem trojanischen Pferd oder von Spyware angegriffen? Dies ist sehr unwahrscheinlich. Viele seriöse Programme verwenden die Loopbackadresse zur Kommunikation zwischen den Komponenten. Zahlreiche persönliche E-Mail- oder Webserver lassen sich beispielsweise über eine Weboberfläche konfigurieren, auf die über die Adresse "http://localhost/" (oder eine vergleichbare Adresse) zugegriffen werden kann.

Firewall lässt Datenverkehr von diesen Programmen zu. Wenn Ereignisse mit der IP-Adresse 127.0.0.1 angezeigt werden, bedeutet dies in der Regel, dass die Quell-IP-Adresse gefälscht ist. Gefälschte Pakete sind oft ein Zeichen dafür, dass jemand nach trojanischen Pferden sucht. Vergessen Sie nicht, dass Firewall diesen Versuch blockiert. Das Erstellen von Berichten zu Ereignissen der IP-Adresse 127.0.0.1 ist offensichtlich nicht hilfreich und daher unnötig.

Das heißt, dass für einige Programme, vor allem Netscape ab Version 6.2 und höher gilt, jedoch dass die Adresse 127.0.0.1 in die Liste **Vertrauenswürdige IP-Adressen** aufgenommen werden muss. Die Komponenten dieser Programme kommunizieren so miteinander, dass Firewall nicht bestimmen kann, ob es sich um einen lokalen Datenverkehr handelt oder nicht.

Bei Netscape 6.2 können Sie zum Beispiel Ihre Buddyliste nicht verwenden, wenn Sie die Adresse 127.0.0.1 nicht als vertrauenswürdig einstufen. Wenn Sie also Datenverkehr von 127.0.0.1 bemerken und alle Anwendungen auf Ihrem Computer normal funktionieren, können Sie diesen Datenverkehr sicherheitshalber blockieren. Sollte jedoch ein Programm (wie Netscape) Probleme haben, nehmen Sie die Adresse 127.0.0.1 in die Liste **Vertrauenswürdige IP-Adressen** in Firewall auf, und ermitteln Sie anschließend, ob das Problem behoben ist.

Wird das Problem durch die Aufnahme von 127.0.0.1 in die Liste **Vertrauenswürdige IP-Adressen** behoben, müssen Sie Ihre Entscheidungsmöglichkeiten abwägen: Wenn Sie die Adresse 127.0.0.1 als vertrauenswürdig einstufen, funktioniert zwar das Programm, allerdings erhöht sich die Gefahr, dass Angriffe mit gefälschten Adressen ausgeführt werden. Wenn Sie diese Adresse nicht als vertrauenswürdig einstufen, funktioniert das Programm nicht. Es wird in diesem Fall jedoch die Gefahr verringert, dass Angriffe mit gefälschten Adressen ausgeführt werden.

Ereignisse von Computern in Ihrem LAN

Für die meisten LAN-Einstellungen in Unternehmen können Sie allen Computern in Ihrem LAN vertrauen.

Ereignisse von privaten IP-Adressen

IP-Adressen im Format 192.168.xxx.xxx, 10.xxx.xxx.xxx und 172.16.0.0 bis 172.31.255.255 werden als nicht routbare oder private IP-Adressen bezeichnet. Diese IP-Adressen sollten Ihr Netzwerk nie verlassen und können in der Regel als vertrauenswürdig angesehen werden.

Der Block 192.168 wird in Zusammenhang mit Microsoft Internet Connection Sharing (ICS) verwendet. Wenn Sie ICS verwenden und Ereignisse von diesem IP-Block angezeigt werden, können Sie die IP-Adresse 192.168.255.255 in die Liste **Vertrauenswürdige IP-Adressen** aufnehmen. Dadurch wird der Block 192.168.xxx.xxx als vertrauenswürdig eingestuft.

Wenn Sie sich nicht in einem privaten Netzwerk befinden und Ereignisse von diesen IP-Bereichen angezeigt werden, bedeutet dies, dass die IP-Quelladresse möglicherweise gefälscht ist. Gefälschte Pakete sind oft ein Zeichen dafür, dass jemand nach trojanischen Pferden sucht. Vergessen Sie nicht, dass Firewall diesen Versuch blockiert.

Da private IP-Adressen von IP-Adressen im Internet getrennt sind, hat das Melden dieser Ereignisse keine Auswirkungen.

ESS (Extended Service Set)

Eine Gruppe von mindestens zwei Netzwerken, die ein Subnetz bilden.

Externe Festplatte

Eine Festplatte, die außerhalb des Computergehäuses aufbewahrt wird.

Firewall

Ein System, das dazu dient, nicht autorisierte Zugriffe auf ein bzw. aus einem privaten Netzwerk zu verhindern. Firewalls können in Form von Hardware, Software oder einer Kombination von beiden implementiert werden. Sie werden häufig verwendet, um zu verhindern, dass nicht autorisierte Internetbenutzer auf private Netzwerke (insbesondere Intranets) zugreifen, die mit dem Internet verbunden sind. Alle Nachrichten, die in das Intranet gelangen oder dieses verlassen, laufen durch eine Firewall. Von dieser werden alle Nachrichten überprüft und jene blockiert, die nicht die angegebenen Sicherheitskriterien erfüllen. Firewalls werden als erste Verteidigungslinie beim Schutz privater Informationen betrachtet. Zur höheren Sicherheit können die Daten verschlüsselt werden.

Freigeben

Ein Vorgang, der es E-Mail-Empfängern ermöglicht, für eine begrenzte Zeit auf ausgewählte gesicherte Dateien zuzugreifen. Wenn Sie eine Datei freigeben, senden Sie die gesicherte Kopie der Datei an die E-Mail-Empfänger, die Sie angeben. Die Empfänger erhalten eine E-Mail der Datensicherung, die ihnen mitteilt, dass Dateien für sie freigegeben wurden. Die E-Mail enthält außerdem einen Link zu den freigegebenen Dateien.

freigegebenes Geheimnis

Siehe auch RADIUS. Schützt den sensiblen Teil von RADIUS-Nachrichten. Der gemeinsame geheime Schlüssel ist ein Kennwort, das von dem Authentifikator und dem Authentifizierungsserver auf eine bestimmte sichere Weise gemeinsam verwendet wird.

Hotspot

Ein bestimmter örtlicher Standort, an dem ein Zugriffspunkt mobilen Besuchern den Zugriff auf öffentliche Breitband-Netzwerkdienste über ein drahtloses Netzwerk ermöglicht. Hotspots befinden sich oft in der Nähe von stark frequentierten Einrichtungen, z. B. Flughäfen, Bahnhöfen, Bibliotheken, Jachthäfen, Messe-Centern und Hotels. Sie haben meist eine geringe Reichweite.

Inhaltsklassifikationsgruppen

Altersgruppen, zu denen ein Benutzer gehört. Der Inhalt wird auf der Grundlage der Inhaltsklassifikationsgruppe bewertet (das bedeutet verfügbar gemacht oder blockiert), zu der der Benutzer gehört. Inhaltsklassifikationsgruppen umfassen Folgendes: kleines Kind, Kind, jüngerer Teenager, älterer Teenager und Erwachsener.

integriertes Gateway

Ein Gerät, in dem die Funktionen eines Zugriffspunkts, Routers und einer Firewall kombiniert sind. Einige Geräte können auch Sicherheitsoptimierungen und Überbrückungsfunktionen enthalten.

Internet

Das Internet besteht aus einer großen Menge verbundener Netzwerke, die TCP/IP-Protokolle zur Ermittlung und Übertragung von Daten verwenden. Ursprünglich ist das Internet aus miteinander verbundenen Universitätscomputern entstanden. Daraus entwickelte sich das Ende der 60er Jahre vom US-Verteidigungsministerium gegründete ARPANET, das als Wegbereiter für das Internet gilt. Heute ist das Internet ein globales Netzwerk von nahezu 100.000 unabhängigen Netzwerken.

Intranet

Ein privates Netzwerk, in der Regel innerhalb einer Organisation, das im Wesentlichen wie das Internet funktioniert. Auf ein Intranet kann auch von externen Computern aus zugegriffen werden, beispielsweise durch Studenten, die auf das Intranet einer Universität, oder externe Mitarbeiter, die auf das Internet eines Unternehmens Zugriff erhalten haben. Firewalls, Anmeldeprozeduren und Kennwörter dienen der Sicherheit eines Intranets.

IP-Adresse

Die IP-Adresse (Internet Protocol Number) ist eine eindeutige Zahlenfolge, deren vier Bestandteile durch Punkte voneinander getrennt sind (z. B. 63.227.89.66). Jeder Internetcomputer verfügt über eine eindeutige IP-Adresse - vom größten Server bis hin zum Laptop, der per Mobilanschluss kommuniziert. Nicht jeder Computer weist einen Domänennamen auf, aber jeder Computer hat eine IP-Adresse.

Im Folgenden werden einige ungewöhnliche Typen von IP-Adressen aufgeführt:

- Nicht routbare IP-Adressen: Diese stellen einen privaten IP-Adressraum dar. Hierbei handelt es sich um IP-Adressen, die im Internet nicht verwendet werden können. Private IP-Blöcke sind 10.x.x.x, 172.16.x.x bis 172.31.x.x und 192.168.x.x.
- Loopback-IP-Adressen**:** Diese Adressen werden zu Testzwecken verwendet. Datenpakete, die an diesen IP-Adressblock gesendet werden, kehren sofort wieder zu dem Gerät zurück, von dem das Paket generiert wurde. Da an diese IP-Adressen gerichtete Datenpakete das Gerät überhaupt nicht verlassen, werden diese Adressen hauptsächlich für Hardware- und Softwaretests verwendet. Der Loopback-IP-Block beginnt mit 127.x.x.x.

Null-IP-Adressen Hierbei handelt es sich um eine ungültige Adresse. Eine Null-IP-Adresse weist darauf hin, dass im Datenverkehr eine leere IP-Adresse verwendet wurde und der Absender den Ursprung des Datenverkehrs nicht preisgeben möchte. Der Absender kann keine Antwort auf den Datenverkehr erhalten, es sei denn, das Paket wird von einer Anwendung empfangen, die den Paketinhalt (d. h. die anwendungsspezifischen Anweisungen) versteht und damit entsprechend umgehen kann. Jede Adresse, die mit 0 beginnt (0.x.x.x), ist eine Null-Adresse. Beispiel: 0.0.0.0 ist eine Null-IP-Adresse.

IP-Spoofing

Das Fälschen der IP-Adressen in einem IP-Paket. Dieses Methode wird in vielen Arten von Angriffen einschließlich dem "Session-Hijacking" verwendet. Sie wird oftmals auch dazu verwendet, die Kopfzeilen von SPAM-E-Mails zu fälschen, damit diese E-Mails nicht mehr zurückverfolgt werden können.

isolieren

Wenn verdächtige Dateien erkannt werden, werden sie isoliert. Sie können dann die entsprechende Aktion ausführen.

Kennwort

Ein (in der Regel alphanumerischer) Code, über den Sie Zugriff auf Ihren Computer bzw. auf ein Programm oder eine Website erhalten.

Kennwort-Tresor

Ein sicherer Speicherbereich für Ihre persönlichen Kennwörter. Er ermöglicht es Ihnen, Ihre Kennwörter sicher zu speichern in dem Wissen, dass kein anderer Benutzer (auch kein McAfee-Administrator oder Systemadministrator) darauf zugreifen kann.

Knoten

Hierbei handelt es sich um einen Computer, der mit einem Netzwerk verbunden ist.

Komprimierung

Ein Vorgang, bei dem Daten (Dateien) in eine Form komprimiert werden, die den zum Speichern oder Übermitteln erforderlichen Platz minimiert.

Kopfzeile

Bei einem Header handelt es sich um Informationen, die im Lauf der Übermittlung zur E-Mail hinzugefügt wurden. Die Kopfzeile bestimmt die Übermittlung der E-Mail durch die Internetsoftware und enthält außerdem die Adresse für die Rückantwort, eine eindeutige Kennung für die E-Mail und andere administrative Angaben. Beispiele für diese Kopfzeilenfelder sind: An, Von, CC, Datum, Betreff, Nachrichten-ID und Empfangen.

LAN (Local Area Network)

Ein Computernetzwerk, dass sich über ein relativ kleines Gebiet erstreckt. Die meisten LANs sind auf ein einzelnes Gebäude oder eine Gruppe von Gebäuden beschränkt. Per Telefonverbindungen oder Funkwellen kann ein LAN aber auch über eine beliebige Entfernung mit anderen LANs verbunden werden. Ein System aus LANs, die auf diese Weise miteinander verbunden sind, wird WAN (Wide-Area Network) genannt. In den meisten LANs werden Workstations und PCs über normale Hubs oder Switches miteinander verbunden. Jeder Knoten (ein einzelner Computer) in einem LAN hat seine eigene CPU, mit der er Programme ausführt, kann aber auch auf Daten und Geräte (z. B. Drucker) im LAN zugreifen. Auf diese Weise können teure Geräte (z. B. Laserdrucker) sowie Daten von vielen Benutzern gemeinsam genutzt werden. Über ein LAN können Benutzer auch miteinander kommunizieren, z. B. E-Mails senden oder an Chat-Sitzungen teilnehmen.

MAC (Media Access Control oder Message Authenticator Code)

Für das Erstgenannte von beiden siehe "MAC-Adresse". Die zweite ausgeschriebene Abkürzung (Message Authenticator Code) bezeichnet einen Code, der zum Identifizieren einer bestimmten Nachricht (z. B. einer RADIUS-Nachricht) verwendet wird. Der Code ist gewöhnlich ein kryptographisch starker Hash des Nachrichteninhalts, der einen eindeutigen Wert als Replay-Schutz enthält.

MAC-Adresse (Media Access Control Address)

Eine Adresse auf unterer Ebene, die einem physikalischen Gerät zugewiesen wird, das auf das Netzwerk zugreift.

MAPI-Konto

Acronym für Messaging Application Programming Interface. Die Microsoft-Schnittstellenspezifikation, die es verschiedenen Messaging- und Arbeitsgruppenanwendungen (einschließlich E-Mail, Voice-Mail und Fax) ermöglicht, einen einzigen Client zu verwenden, wie den Exchange-Client. MAPI wird daher häufig in Unternehmensumgebungen mit Microsoft® Exchange Server eingesetzt. Zahlreiche Benutzer verwenden allerdings Microsoft Outlook für persönliche Internet-E-Mails.

MSN-Konto

Acronym für Microsoft Network. Ein Online-Dienst und Internetportal. Dies ist ein webbasiertes Konto.

Netzwerk

Ein Netzwerk entsteht durch die Verbindung von mehreren Computern.

Netzwerk-Laufwerk

Ein Disketten- oder Band-Laufwerk, das mit einem Server in einem Netzwerk verbunden ist, das für mehrere Benutzer freigegeben ist. Netzwerk-Laufwerke werden gelegentlich auch als Remote-Laufwerke bezeichnet.

Netzwerkzuordnung

In Network Manager ist die Netzwerkzuordnung eine graphische Darstellung des Computers und der Komponenten, die Ihr privates Netzwerk ausmachen.

NIC (Network Interface Card, Netzwerkkarte)

Eine Karte, die in ein Notebook oder ein anderes Gerät gesteckt wird und das Gerät mit dem LAN verbindet.

Online-Sicherungs-Repository

Der Speicherort auf dem Online-Server, an dem Ihre überwachten Dateien nach der Sicherung gespeichert werden.

Parental controls

Einstellungen, die das Konfigurieren von Inhaltsklassifikationen und Internetzugriffszeiten ermöglichen. Darin wird festgelegt, welche Inhalte und Websites ein Benutzer anzeigen kann und wann und wie lange dieser Benutzer auf das Internet zugreifen kann. Mit Kindersicherungen können Sie außerdem allgemeine Beschränkungen für den Zugriff auf bestimmte Websites festlegen oder den Zugriff auf der Grundlage von Altersgruppen und Stichwörtern gewähren oder blockieren.

PCI-Drahtlosadapter-Karte

Verbindet einen Desktopcomputer mit einem Netzwerk. Die Karte wird in einen PCI-Erweiterungssteckplatz im Computer gesteckt.

Phishing

Als "Fishing" ausgesprochen, ist ein Scam, mithilfe dessen Ihnen wertvolle Informationen, wie Ihre Kreditkarten- und Sozialversicherungsnummer, Benutzer-IDs und Kennwörter gestohlen werden sollen. Eine offiziell aussehende E-Mail wird an potentielle Opfer gesendet. Dabei wird behauptet, die Mail stamme vom ISP, der Bank oder einem Geschäft, bei dem die Benutzer einkaufen. E-Mails können an Personen auf ausgewählten oder beliebigen Listen gesendet werden, in der Erwartung, dass ein gewisser Prozentsatz der Empfänger tatsächlich über ein Konto bei dem echten Unternehmen verfügt.

POP3-Konto

Acronym für Post Office Protocol 3. Die meisten privaten Benutzer haben diesen Kontotyp. Dies ist die aktuelle Version des Post Office Protocol-Standards, der häufig in TCP/IP-Netzwerken verwendet wird. Auch bekannt als standardmäßiges E-Mail-Konto.

Popups

Kleine Fenster, die über anderen Fenstern auf dem Bildschirm angezeigt werden. Popup-Fenster werden oft in Webbrowsern verwendet, um Werbung anzuzeigen. McAfee blockiert Popup-Fenster, die automatisch geladen werden, wenn eine Webseite in Ihrem Browser geladen wird. Popup-Fenster, die geladen werden, wenn Sie auf einen Link klicken, werden von McAfee nicht blockiert.

Potentiell unerwünschtes Programm

Potentiell unerwünschte Programme umfassen Spyware, Adware und andere Programme, die Ihre Daten ohne Ihre Zustimmung sammeln und übertragen.

PPPoE

Abkürzung für "Point-to-Point Protocol Over Ethernet". PPPoE wird von vielen DSL-Providern verwendet und unterstützt die in PPP häufig verwendeten Protokollebenen und Authentifizierung. Mit PPPoE kann eine Punkt-zu-Punkt-Verbindung in der normalen Multipoint-Ethernet-Architektur hergestellt werden.

Protokoll

Ein vorab vereinbartes Format zum Übertragen von Daten zwischen zwei Geräten. Aus Sicht des Benutzers besteht der einzige interessante Aspekt bei Protokollen darin, dass der Computer oder das Gerät die entsprechenden Protokolle unterstützen muss, um mit einem jeweils anderen Computer kommunizieren zu können. Das Protokoll kann entweder in der Hardware oder in der Software implementiert sein.

Proxy

Ein Computer (oder die auf ihm ausgeführte Software), der als Barriere zwischen einem Netzwerk und dem Internet fungiert, indem er gegenüber externen Sites nur als eine einzige Netzwerkadresse auftritt. Indem er für alle internen Computer eine Zwischenwand darstellt, schützt der Proxy Netzwerkidentitäten und ermöglicht gleichzeitig Zugriff auf das Internet. Siehe auch Proxyserver.

Proxy-Server

Eine Firewallkomponente, die den ein- und ausgehenden Internetverkehr eines LAN (Local Area Network) verwaltet. Ein Proxyserver kann durch Liefern häufig angeforderter Daten, z.B. einer beliebten Webseite, die Leistung steigern und Anforderungen filtern, die der Eigentümer als nicht geeignet einstuft, z.B. Anforderungen nach unautorisiertem Zugriff auf proprietäre Dateien.

Pufferüberlauf

Pufferüberläufe finden statt, wenn verdächtige Programme oder Prozesse versuchen, mehr Daten in einem Puffer (Speicherbereich für temporäre Dateien) auf Ihrem Computer zu speichern als erlaubt, so dass gültige Daten in nahegelegenen Puffern beschädigt oder überschrieben würden.

RADIUS (Remote Access Dial-In User Service)

Ein Protokoll zum Authentifizieren von Benutzern, meist im Zusammenhang mit Remote-Zugriff. Ursprünglich definiert für den Einsatz in RAS-Einwahl-Servern, wird das Protokoll heutzutage in einer breiten Vielzahl von Authentifizierungsumgebungen genutzt, einschließlich der 802.1x-Authentifizierung des gemeinsamen geheimen Schlüssels von WLAN-Benutzern.

Reiner Text

Nachrichten, die nicht verschlüsselt sind.

Roaming

Die Fähigkeit, aus dem Empfangsbereich eines Zugriffspunkts in den eines anderen zu wechseln, ohne dass dabei der Betrieb unterbrochen oder die Verbindung verloren wird.

Router

Ein Netzwerkgerät, das Pakete von einem Netzwerk in ein anderes weiterleitet. Router lesen jedes eingehende Paket und entscheiden anhand interner Routingtabellen, wie das Paket weitergeleitet werden soll. Die Wahl der Schnittstelle, an die ausgehende Pakete gesendet werden, kann davon abhängen, in welcher Konstellation Quell- und Zieladresse miteinander stehen, oder sich nach den aktuellen Gegebenheiten im Netzwerkverkehr (z. B. Auslastung, Leitungskosten oder ausgefallene Leitungen) richten. Für "Router" wird manchmal auch der Begriff "Zugriffspunkt" verwendet.

Schlüssel

Eine Folge von Buchstaben und/oder Zahlen, mit der zwei Geräte ihre Kommunikation miteinander authentifizieren können. Dabei müssen beide Geräte über den Schlüssel verfügen. Siehe auch WEP, WPA, WPA2, WPA-PSK und WPA2- PSK.

Schnellarchivierung

Die Archivierung nur der überwachten Dateien, die seit der letzten vollständigen Archivierung oder Schnellarchivierung geändert wurden.

Schwarze Liste

Eine Liste der Websites, die als schädlich angesehen werden. Eine Website kann in eine schwarze Liste eingetragen werden, wenn über sie betrügerische Handlungen vorgenommen werden oder wenn sie Browser-Schwachstellen ausnutzt, um potentiell unerwünschte Programme an den Benutzer zu senden.

Server

Hierbei handelt es sich um einen Computer oder eine Software, der/die bestimmte Dienste für das Ausführen einer Software auf anderen Computern zur Verfügung stellt. Der "E-Mail-Server" bei Ihrem ISP ist eine Software, die den gesamten eingehenden und ausgehenden E-Mail-Datenverkehr für alle Benutzer des ISPs verarbeitet. Bei einem Server auf einem LAN handelt es sich um eine Hardware, die den primären Knoten im Netzwerk darstellt. Diese Hardware kann wiederum Software enthalten, die den zugehörigen Clientcomputern bestimmte Dienste, Daten oder andere Funktionen zur Verfügung stellt.

sichern

Verwenden Sie diese Option, um eine Kopie Ihrer überwachten Dateien auf einem sicheren Online-Server zu erstellen.

Skript

Skripts können Dateien erstellen, kopieren oder löschen. Sie können auch Ihre Windows-Registrierung öffnen.

SMTP-Server

Acronym für Simple Mail Transfer Protocol. Ein TCP/IP-Protokoll, das für das Senden von Nachrichten von einem Computer an einen anderen in einem Netzwerk verwendet wird. Dieses Protokoll wird im Internet verwendet, um E-Mails weiterzuleiten.

Speicherort für die oberflächliche Überwachung

Ein Ordner auf Ihrem Computer, der von der Datensicherung auf Änderungen überwacht wird. Wenn Sie einen Speicherort für die oberflächliche Überwachung einrichten, sichert die Datensicherung die überwachten Dateitypen innerhalb dieses Ordners, nicht aber innerhalb der Unterordner.

Speicherort für umfassende Überwachung

Ein Ordner (und alle Unterordner) auf Ihrem Computer, der von Data Backup auf Änderungen hin überwacht wird. Wenn Sie einen Speicherort für die umfassende Überwachung festlegen, sichert Data Backup die überwachten Dateitypen in diesem Order und seinen Unterordnern.

SSID (Service Set Identifier)

Der Netzwerkname für die Geräte in einem Funk-LAN-Subsystem. Das ist eine Zeichenfolge aus 32 Zeichen, die im Klartext steht und zum Kopf jedes WLAN-Pakets hinzugefügt wird. Die SSID unterscheidet WLANs voneinander. Daher müssen alle Benutzer eines Netzwerks dieselbe SSID angeben, um auf einen bestimmten Zugriffspunkt zuzugreifen. Mit einer SSID wird der Zugriff von Clientgeräten verhindert, die eine andere SSID besitzen. Die SSID wird jedoch von Zugriffspunkten standardmäßig zusammen mit dem Signal übertragen. Dadurch kann ein Hacker die SSID per "Sniffing" selbst dann ermitteln, wenn die SSID-Übertragung deaktiviert ist.

SSL (Secure Sockets Layer)

Ein von Netscape entwickeltes Protokoll zum Übermitteln vertraulicher Dokumente über das Internet. SSL arbeitet mit einem öffentlichen Schlüssel, mit dem die Daten verschlüsselt werden, die über die SSL-Verbindung übertragen werden. SSL wird sowohl von Netscape Navigator als auch von Internet Explorer genutzt und unterstützt. Viele Websites verwenden dieses Protokoll, wenn Benutzer vertrauliche Informationen (z. B. Kreditkartennummern) eingeben müssen. Laut Konvention beginnen URLs, die eine SSL-Verbindung erfordern, mit der Zeichenfolge "https:" anstelle von "http:".

Standard-E-Mail-Konto

Dies ist die am häufigsten vorkommende Kontoart. Siehe auch POP3-Konto.

Stichwort

Ein Wort, das Sie einer gesicherten Datei zuordnen können, um eine Beziehung oder Verbindung mit anderen Dateien aufzubauen, denen dasselbe Stichwort zugeordnet ist. Durch das Zuordnen von Stichwörtern zu Dateien ist es einfacher, nach Dateien zu suchen, die Sie im Internet veröffentlicht haben.

Synchronisieren

Zur Behebung von Inkonsistenzen zwischen gesicherten Dateien und den auf Ihrem lokalen Computer gespeicherten Dateien. Sie synchronisieren Dateien, wenn die Version der Datei im Online-Sicherungs-Repository aktueller als die Version der Datei auf den anderen Computern ist. Durch die Synchronisierung wird die Kopie der Datei auf Ihren Computern mit der Version der Datei im Online-Sicherungs-Repository aktualisiert.

SystemGuard

SystemGuards erkennt nicht autorisierte Änderungen auf Ihrem Computer und gibt ggf. eine Warnung aus.

TKIP (Temporal Key Integrity Protocol)

Eine schnelle Methode zum Lösen der konstruktionsbedingten Sicherheitsschwächen von WEP, speziell des Problems der Wiederverwendung von Verschlüsselungsschlüsseln. Bei TKIP werden temporäre Schlüssel nach jeweils 10.000 Paketen geändert. Auf diese Weise wird eine dynamische Verteilungsmethode erzielt, die die Sicherheit des Netzwerks beträchtlich erhöht. Der TKIP-Sicherheitsprozess beginnt mit einem temporären 128-Bit-Schlüssel, der von Clients und Zugriffspunkten gemeinsam verwendet wird. TKIP kombiniert diesen temporären Schlüssel mit der MAC-Adresse (des Clientcomputers) und fügt dann einen relativ großen Initialisierungsvektor (16 Oktetts) hinzu, um den Schlüssel zu erstellen, mit dem die Daten verschlüsselt werden. Durch diese Vorgehensweise wird sichergestellt, dass jede Station ihre Daten mit einem anderen Schlüssel-Stream verschlüsselt. TKIP führt die Verschlüsselung mit RC4 durch. WEP verwendet ebenfalls RC4.

Trojaner

Trojaner sind Programme, die sich als gutartige Anwendungen "tarnen". Trojaner sind keine Viren, da sie sich nicht fortpflanzen, können Ihrem Computer jedoch einen ähnlich Schaden zufügen wie Viren.

Überwachte Dateitypen

Die Dateitypen (beispielsweise .DOC, .XLS usw.), die von der Datensicherung innerhalb der Überwachungs-Speicherorte gesichert oder archiviert werden.

Überwachungs-Speicherorte

Die Ordner auf Ihrem Computer, die von der Datensicherung überwacht werden.

Unerwünschte Zugriffspunkte

Ein Zugriffspunkt, den ein Unternehmen für den Betrieb nicht autorisiert. Das Problem dabei ist, dass nicht autorisierte Zugriffspunkte oft nicht den Sicherheitsrichtlinien für WLANs (Wireless LAN, Funk-LAN) entsprechen. Ein nicht autorisierter Zugriffspunkt bietet eine offene, unsichere Schnittstelle in das Unternehmensnetzwerk von außerhalb der physikalisch kontrollierten Einrichtung.

In einem ordnungsgemäß gesicherten WLAN richten nicht autorisierte Zugriffspunkte mehr Schäden an als nicht autorisierte Benutzer. Wenn wirksame Authentifizierungsmechanismen vorhanden sind, müssen nicht autorisierte Benutzer beim Versuch, auf ein WLAN zuzugreifen, nicht unbedingt auch an wertvolle Ressourcen des Unternehmens gelangen. Zu größeren Problemen kommt es jedoch, wenn sich ein Mitarbeiter oder Hacker über den nicht autorisierten Zugriffspunkt anmeldet. Ein nicht autorisierter Zugriffspunkt erlaubt praktisch jedem, der über ein 802.11-kompatibles Gerät verfügt, den Zutritt in das Unternehmensnetzwerk. Dadurch gelangt man schnell sehr nah an geschäftskritische Ressourcen.

URL

Uniform Resource Locator. Hierbei handelt es sich um das Standardformat für Internetadressen.

USB-Drahtlosadapter-Karten

Eine erweiterbare serielle Schnittstelle mit Plug-and-Play-Funktionalität. Diese Schnittstelle bietet eine standardisierte und preisgünstige drahtlose Anschlussmöglichkeit für Peripheriegeräte wie Tastaturen, Mäuse, Joysticks, Drucker, Scanner, Speichergeräte und Videokameras.

Veröffentlichen

Eine gesicherte Datei öffentlich im Internet verfügbar machen.

Verschlüsselung

Ein Vorgang, bei dem Daten von Text in Code umgewandelt werden, wodurch die Informationen verschleiert werden, so dass Personen, die den Code nicht entschlüsseln können, sie nicht lesen können.

Verwaltetes Netzwerk

Ein privates Netzwerk mit zwei Arten von Mitgliedern: verwaltete Mitglieder und unverwaltete Mitglieder. Verwaltete Mitglieder erlauben es anderen Computern im Netzwerk, ihren McAfee-Schutzstatus einzusehen, unverwaltete Mitglieder tun das nicht.

Vollständige Archivierung

Die Archivierung eines kompletten Datensatzes basierend auf den von Ihnen festgelegten überwachten Dateitypen und Speicherorten.

VPN (Virtual Private Network)

Ein Netzwerk, das entsteht, indem Knoten unter Verwendung von öffentlichen Leitungen neu miteinander verbunden werden. Es gibt zum Beispiel eine Reihe von Systemen, mit denen Sie Netzwerke erstellen können, die das Internet als Medium für den Datentransport verwenden. Diese Systeme setzen Verschlüsselung und andere Sicherheitsmechanismen ein, um sicherzustellen, dass nur autorisierte Benutzer auf das Netzwerk zugreifen und die Daten nicht abgefangen werden können.

Wardriver

Das sind mit Notebooks bewaffnete Eindringlinge, die mit spezieller Software und modifizierter Hardware durch die Gegend streifen, um Datenverkehr von Funk-LANs abzufangen.

Web-Bugs

Kleine Grafikdateien, die sich selbst in Ihre HTML-Seiten einbetten können und es einer nicht autorisierten Quelle erlauben, Cookies auf Ihrem Computer zu platzieren. Diese Cookies können dann Informationen an die nicht autorisierte Quelle übertragen. Web-Bugs sind auch als Web-Beacons, Pixel-Tags, durchsichtige GIFs oder unsichtbare GIFs bekannt.

Weiße Liste

Eine Liste der Websites, denen der Zugriff erlaubt wird, da sie nicht als betrügerische Websites angesehen werden.

WEP (Wired Equivalent Privacy)

Ein Verschlüsselungs- und Authentifizierungsprotokoll aus dem Standard 802.11. Die anfänglichen Versionen basieren auf RC4-Verschlüsselungen und haben beträchtliche Schwächen. Der Sicherheitsansatz von WEP besteht darin, dass per Funk übertragene Daten verschlüsselt werden, damit sie geschützt sind, wenn sie von einem Endpunkt zum anderen übertragen werden. Es hat sich jedoch herausgestellt, dass WEP nicht so sicher ist, wie man ursprünglich angenommen hatte.

Wi-Fi (Wireless Fidelity)

Dieser Begriff wird allgemein für alle Arten von 802.11-kompatiblen Netzwerken verwendet, sei es 802.11b, 802.11a, Dual-Band usw. Der Begriff wird von der Wi-Fi Alliance verwendet.

Wi-Fi Alliance

Eine Organisation, die aus führenden Anbietern von drahtloser Hardware und Software besteht und deren Ziel darin liegt, (1) allen 802.11-basierten Produkten die gegenseitige Kompatibilität zu zertifizieren und (2) den Begriff "Wi-Fi" in allen Märkten für Produkte für 802.11-basierte Funk-LANs als globalen Markennamen zu fördern. Die Organisation dient als Konsortium, Testlabor und Clearinghouse für Anbieter, die die gegenseitige Kompatibilität und das Wachstum dieser Branche voranbringen möchten.

Auch wenn alle Produkte der Standards 802.11a/b/g als Wi-Fi bezeichnet werden, dürfen nur die Produkte, die den Test der Wi-Fi Alliance bestanden haben, das Prädikat "Wi-Fi Certified" (eine eingetragene Marke) tragen. Produkte, die den Test erfolgreich bestanden haben, müssen ein Identifikationssiegel auf ihrer Verpackung haben, auf dem "Wi-Fi Certified" sowie das verwendete Funkfrequenzband stehen. Die Wi-Fi Alliance war früher unter der Bezeichnung Wireless Ethernet Compatibility Alliance (WECA) bekannt, änderte jedoch im Oktober 2002 ihren Namen, um die Marke "Wi-Fi" besser darstellen zu können, deren Aufbau das Ziel der Gruppe ist.

Wi-Fi Certified

Produkte, die von der Wi-Fi Alliance getestet und als Wi-Fi Certified (eine eingetragene Marke) zugelassen wurden, sind als miteinander vollständig kompatibel zertifiziert, auch wenn sie von unterschiedlichen Herstellern stammen. Ein Benutzer eines Produkts mit dem Prädikat "Wi-Fi Certified" kann einen Zugriffspunkt einer beliebigen Marke zusammen mit Clienthardware anderer Marken, die ebenfalls zertifiziert sind, verwenden. Üblicherweise funktionieren Wi-Fi-Produkte mit allen anderen Produkten zusammen, die dieselbe Funkfrequenz verwenden (z. B. 2,4 GHz bei 802.11b oder 11g; 5 GHz bei 802.11a), auch wenn diese nicht das Prädikat "Wi-Fi Certified" haben.

Wiederherstellen

Abrufen einer Kopie einer Datei aus dem Online-Sicherungs-Repository oder einem Archiv.

WLAN (Wireless Local Area Network)

Siehe auch LAN. Ein LAN, das ein drahtloses Medium zum Verbinden verwendet. In WLANs erfolgt die Kommunikation zwischen den Knoten über hochfrequente Funkwellen anstelle von Kabeln.

Wörterbuchangriff

Bei diesen Angriffen wird versucht, ein Kennwort zu ermitteln, indem unzählige Wörter aus einer Liste durchprobiert werden. Dabei geben die Angreifer diese Wörter und alle ihre Kombinationen nicht selbst manuell ein, bis sie das Kennwort von jemandem ermittelt haben, sondern verwenden dafür Tools, die diesen Vorgang automatisieren.

WPA (Wi-Fi Protected Access)

Ein Spezifikationsstandard, der das Niveau von Datenschutz und Zugriffskontrolle bei vorhandenen und zukünftigen Funk-LAN-Systemen stark erhöht. WPA ist vom Standard IEEE 802.11i abgeleitet und damit kompatibel und für die Ausführung auf vorhandener Hardware in Form eines Softwareupgrade entworfen. Bei korrekter Installation bietet es Benutzern von Funk-LANs ein hohes Maß an Sicherheit dafür, dass ihre Daten geschützt bleiben und nur autorisierte Netzwerkbenutzer auf das Netzwerk zugreifen können.

WPA-PSK

Ein spezieller WPA-Modus, der für Privatanwender entworfen wurde, die keine starke Sicherheit wie in Unternehmen üblich benötigen und keinen Zugriff auf Authentifizierungsserver haben. In diesem Modus kann der Privatanwender das Startkennwort manuell eingeben, um WPA im PSK-Modus zu aktivieren, und sollte die Passphrase auf jedem drahtlosen Computer und Zugriffspunkt regelmäßig ändern. Siehe auch WPA2-PSK und TKIP.

WPA2

Siehe auch WPA. WPA2 ist eine Aktualisierung des WPA-Sicherheitsstandards und basiert auf dem 802.11i IEEE-Standard.

WPA2-PSK

Siehe auch WPA-PSK und WPA2. WPA2-PSK ist WPA-PSK ähnlich und basiert auf dem WPA2-Standard. Eine häufig verwendete Funktion von WPA2-PSK ist, dass Geräte häufig mehrere Verschlüsselungsmodi (z. B. AES, TKIP) gleichzeitig unterstützten, während ältere Geräte üblicherweise nur jeweils einen Verschlüsselungsmodus unterstützten (d. h., alle Clients müssten denselben Verschlüsselungsmodus unterstützen).

Wurm

Würmer sind sich selbst replizierende Viren, die sich im Arbeitsspeicher eines Computers befinden und Kopien von sich selbst per E-Mail verbreiten. Würmer replizieren und verbrauchen Systemressourcen, wodurch die Leistung herabgesetzt und Tasks angehalten werden.

Zugriffspunkt

Ein Netzwerkgerät, das 802.11-kompatiblen Clients die Verbindung zu einem LAN (Local Area Network) ermöglicht. Zugriffspunkte erweitern die physikalische Betriebsreichweite für drahtlose Benutzer. Sie werden auch als drahtlose Router bezeichnet.

Info zu McAfee

McAfee, Inc., mit Hauptsitz in Santa Clara, Kalifornien (USA), ist Marktführer im Bereich Intrusion Prevention und Security Risk Management und bietet weltweit präventive und bewährte Lösungen und Services zum Schutz von Systemen und Netzwerken. Dank der unübertroffenen Sicherheitsexpertise von McAfee und seiner Verpflichtung zur Innovation sind private Nutzer, Unternehmen, der öffentliche Sektor und Service Provider in der Lage, Angriffe abzuwehren, Störungen zu vermeiden und ihre Sicherheit kontinuierlich zu verfolgen und zu verbessern.

Copyright

Copyright i 2006 McAfee, Inc. Alle Rechte vorbehalten. Kein Teil dieser Veröffentlichung darf ohne schriftliche Erlaubnis von McAfee, Inc. in irgendeiner Form oder mit irgendwelchen Mitteln vervielfältigt, übertragen, transkribiert, in einem Informationsabrufsystem gespeichert oder in eine andere Sprache übersetzt werden. McAfee und andere hier erwähnten Marken sind eingetragene Marken oder Marken von McAfee, Inc. und/oder Tochtergesellschaften in den USA und/oder anderen Ländern. Die Farbe Rot in Verbindung mit Sicherheit steht unverkennbar für alle McAfee Markenprodukte. Alle anderen hier erwähnten eingetragenen und nicht eingetragenen Marken und unter Copyright stehenden Materialien sind ausschließlich Eigentum ihrer jeweiligen Inhaber.

MARKEN

ACTIVE FIREWALL, ACTIVE SECURITY, ACTIVESECURITY (UND IN KATAKANA), ACTIVESHIELD, ANTIVIRUS ANYWARE UND DESIGN, CLEAN-UP, DESIGN (STILISIERTES E), DESIGN (STILISIERTES N), ENTERCEPT, ENTERPRISE SECURECAST, ENTERPRISE SECURECAST (UND IN KATAKANA), EPOLICY ORCHESTRATOR, FIRST AID, FORCEFIELD, GMT, GROUPSHIELD, GROUPSHIELD (UND IN KATAKANA), GUARD DOG, HOMEGUARD, HUNTER, INTRUSHIELD, INTRUSION PREVENTION THROUGH INNOVATION, M UND DESIGN, MCAFEE, MCAFEE (UND IN KATAKANA), MCAFEE UND DESIGN, MCAFEE.COM, MCAFEE VIRUSSCAN, NA NETWORK ASSOCIATES, NET TOOLS, NET TOOLS (UND IN KATAKANA), NETCRYPTO, NETOCTOPUS, NETSCAN, NETSHIELD, NETWORK ASSOCIATES, NETWORK ASSOCIATES COLLISEUM, NETXRAY, NOTESGUARD, NUTS & BOLTS, OIL CHANGE, PC MEDIC, PCNOTARY, PRIMESUPPORT, QUICKCLEAN,RINGFENCE, ROUTER PM, SECURECAST, SECURESELECT, SPAMKILLER, STALKER, THREATSCAN, TIS, TMEG, TOTAL VIRUS DEFENSE, TRUSTED MAIL, UNINSTALLER, VIREX, VIRUS FORUM, VIRUSCAN, VIRUSSCAN, VIRUSSCAN (UND IN KATAKANA), WEBSCAN, WEBSHIELD, WEBSHIELD (UND IN KATAKANA), WEBSTALKER, WEBWALL, WHAT'S THE STATE OF YOUR IDS?, WHO'S WATCHING YOUR NETWORK, YOUR E-BUSINESS DEFENDER, YOUR NETWORK. OUR BUSINESS.

Index

8

802.11 404
802.11a....404
802.11b 404
802.11g....404
802.1x....405

A

Abrufen des Administratorkennworts ...30
Abrufen einer übersicht über die Archivierungsvorgänge 298
Aktiveren der Filterung von Web-Mail-Konten 207
Aktivieren des Phishing-Schutzes 236
Aktivieren des Spam-Schutzes 232
Aktivieren des Spyware-Schutzes....86
Aktivieren des Virenschutzes....83
Aktivieren einer Symbolleiste 233
Aktivieren von SystemGuards....87
Aktualisieren der Firmware des Routers oder Zugriffspunkts....369
Aktualisieren des drahtlosen Adapters 376
Aktuelle Schlüssel anzeigen 344, 368
Akzeptieren einer Datei von einem anderen Computer....397, 398
Allgemeines zu SystemGuards für Programme 89
Allgemeines zu Warnungen 128
An geschützten drahtlosen Netzwerken anmelden 307, 310, 331, 372
Andere Probleme 379
Ändern der Anzeigeeigenschaften eines Geräts 74
Ändern der Berechtigungen eines verwalteten Computers 73
Ändern der Filterstufe für E-Mail-Nachrichten 216
Ändern der Filterung von E-Mail-Nachrichten 216
Ändern der Liste 264
Ändern der Vorgehensweise, wie Nachrichten verarbeitet werden 218
Ändern der Vorgehensweise, wie Nachrichten verarbeitet werden 218
Ändern des Administratorkennworts....30
Ändern des Archiv-Speicherorts....285
Ändern einer blockierten Website 258
Ändern einer Website in der Liste der abgelehnten Cookies eines Benutzers 254
Ändern einer Website in der Liste der akzeptierten Cookies eines Benutzers 251
Ändern einer zulässigen Website 262
Ändern eines Kennworts im Kennwort-Tresor....275
Ändern spezieller Filter....217
Ändern von Filteroptionen....215
Ändern von Phishing-Filteroptionen...237
Ändern von Web-Mail-Konten....204
Anmelden am verwalteten Netzwerk....65
Anmelden an einem verwalteten Netzwerk.... 65, 387, 391
Anschluss 405
Anzahl der monatlich geschützten Computer ansehen 360, 361, 362, 364
Anzahl der Schlüsselrotationen einsehen 344, 345, 346, 347, 349, 361
Anzahl der täglichen Verbindungen ansehen 360, 362, 364
Anzeigen der Elementdetails....64
Anzeigen der SecurityCenter-Informationen 22
Anzeigen oder Verbergen von Elementen in der Netzwerkzuordnung 64
Anzeigen von Informationen zum installierten Produkt 22
Anzeigen von Protokollen für gefilterte Web-Mail 208
Anzeigen zuletzt aufg. Ereignisse und Protokolle....111
Arbeiten mit archivierten Dateien 291
Arbeiten mit der Netzwerkzuordnung...62
archivieren 405
Archivieren von Dateien 281
Auf welchen Computern muss diese Software installiert werden?....366
Aufforderung zur Eingabe des WEP-, WPA- oder WPA2-Schlüssels....375
Aufnehmen eines Speicherorts in das Archiv....283
Ausführen häufiger Tasks 39

Ausführen von vollständigen Archivierungen und Schnellarchivierungen.....287
Ausgehende Ereignisse anzeigen 150, 151, 153, 154, 157, 160, 183
Ausschließen eines Speicherorts aus dem Archiv.....285
Auswahl eines anderen Sicherheitsmodus 381
Authentifizierung.....405
Autom. Melden anonymer Informationen 112
Automatische Schlüsselrotation aussetzen 331, 346, 348, 374, 375
Automatisches Aktualisieren von Freunden 212
Automatisches Beheben von Sicherheitsproblemen 21
Automatisches Herunterladen und Installieren von Updates 32
Automatisches Herunterladen von Updates.....32, 33
Automatisches Prüfen auf Updates.....32
Automatisches Warten Ihres Computers 41

B

Bandbreite.....405
Bearbeiten eines POP3- oder MSN/Hotmail-Web-Mail-Kontos 204
Bearbeiten von Adressbüchern 213
Bearbeiten von Freunden 211
Bearbeiten von persönlichen Filtern ...223
Beheben von Sicherheitslücken 75
Beheben von Sicherheitsproblemen.....21
Bei McAfee melden.....112
Bei Verwendung anderer Programme lautet der Netzwerkname anders.....379
Benachrichtigen vor dem Herunterladen von Updates.....32, 34
Benachrichtigung bei gesendeter Datei erhalten.....398
Bereinigen Ihres Computers.....47
Bevorzugte drahtlose Netzwerke entfernen 326, 327
Bevorzugte Netzwerke auflisten...326, 327
Bibliothek.....405
Bilderanalyse.....406
Bin ich geschützt?.....15
Blockieren einer Website 258
Blockieren potentiell anstößiger Bilder 265
Blockieren potentiell anstößiger Web-Bilder.....265
Blockieren von Anzeigen 268
Blockieren von Anzeigen, Popups und Web-Bugs 268
Blockieren von persönlichen Informationen..... 270, 271
Blockieren von Popups 269
Blockieren von Web-Bugs.....269
Blockieren von Websites..... 257, 261
Blockieren von Websites auf der Grundlage von Stichwörtern..... 246, 260
Browser 406
Brute-Force-Angriff.....406

C

chiffrierter Text.....406
Client.....406
Computer aus dem Protokoll 177, 178, 182, 184, 188, 189
Computer im Netzwerk nicht mehr als vertrauenswürdig einstufen.....69
Computer während des Hochfahrens schützen 141
Computer zum geschützten drahtlosen Netzwerk hinzufügen 309, 315, 319, 372, 375
Computern administrativen Zugriff gewähren 307, 316
Computerverbindungen verwalten 167
Cookie 407
Copyright 424

D

Dateien freigeben.....394
Dateien freigeben und senden.....393
Dauer der Netzwerkverbindung ansehen 354, 355, 356, 357, 358, 359
De-/Aktivieren des Phishing-Schutzes 236
Deaktivieren der Filterung von Web-Mail-Konten 207
Deaktivieren der Verschlüsselung und Komprimierung für Archive.....286
Deaktivieren des Phishing-Schutzes....236
Deaktivieren des Spyware-Schutzes.....86
Deaktivieren einer Symbolleiste 233
Deaktivieren von automatischen Updates 32, 34, 36
Deaktivieren von Stichwort-Scans.....259
Deaktivieren von SystemGuards.....87
Defragmentieren von Dateien und Ordnern 43
Dem Netzwerk beitreten.....388
Denial of Service, DoS.....407
Derzeit geschützte Computer ansehen 325, 361, 362, 364

Die Sicherheitsstufe..... 135, 136, 137, 145
DNS.....408
DNS-Server 408
Domäne.....408
Download schlägt auf sicherem Netzwerk fehl.....368
Drahtlose Netzwerke schützen.....305
Drahtlose Netzwerke überwachen.....353
Drahtlose Netzwerkverbindungen überwachen .354, 355, 356, 357, 358, 359
Drahtlose Router oder Zugriffspunkte entfernen 331, 333, 368, 372
Drahtlose Router oder Zugriffspunkte konfigurieren.....380
Drahtlosen Netzwerken verwalten.....323
Drahtloser Adapter.....408
Drucker freigeben.....399

E

EasyNetwork einrichten.....385
EasyNetwork starten 386
Echtzeit-Scans 408
Ein Element kann auch nach dem Neustart nicht entfernt werden.....118
Ein Virus kann nicht bereinigt oder gelöscht werden 118
Eine Bedrohung wurde erkannt. Wie soll ich vorgehen?.....116
Eine Datei an einen anderen Computer senden.....397
Eingehende Ereignisse anzeigen ..182, 188
Eingehenden und ausgehenden Datenverkehr analysieren 192, 193
Einladen eines Computers, sich am verwalteten Netzwerk anzumelden 67
Einrichten der Kindersicherung.....245
Einrichten des Kennwort-Tresors 274
Einstellungen für ICMP-Echo-Request-Anforderungen konfigurieren.....141
E-Mail.....408
E-Mail-Client 408
E-Mail-Schutz aktivieren 98
E-Mail-Schutz deaktivieren 98
E-Mail-Schutz konfigurieren 99, 117
Empfehlungen aktivieren 138
Empfehlungen deaktivieren 139
Empfehlungen für Warnungen konfigurieren 138
Entfernen einer blockierten Website ...259
Entfernen einer Website aus der Liste der abgelehnten Cookies eines Benutzers 255
Entfernen einer Website aus der Liste der akzeptierten Cookies eines Benutzers 252
Entfernen einer zulässigen Website.....262
Entfernen eines Kennworts aus dem Kennwort-Tresor.....276
Entfernen nicht verwendeter Dateien und Ordner.....42
Entfernen persönlicher Filter 224
Entfernen von Adressbüchern.....213
Entfernen von Dateien aus der Liste....297
Entfernen von Freunden 211
Entfernen von unter Quarantäne gestellten Programmen, Cookies und Dateien 109
Entfernen von Web-Mail-Konten 206
Ereignis 409
Ereignisprotokolleinstellungen konfigurieren.....180
Ereignisprotokollierung 170, 177, 178, 180
Ereignisse anzeigen.....111
Erkennung von Intrusionsversuchen konfigurieren.....142
Erläuterung der Network Manager-Symbole 59
Erläuterungen zu den Funktionen von Shredder 52
Erläuterungen zu den QuickClean-Funktionen.....46
Erläuterungen zu den Schutzkategorien und -typen 16
Erläuterungen zu den SecurityCenter-Symbolen 13
Erläuterungen zu E-Mail- und IM-Schutz 19
Erläuterungen zum Parental Controls-Schutz 20
Erläuterungen zum Schutz von Computer und Dateien.....17
Erläuterungen zum Schutz von Internet und Netzwerk.....18
Erläuterungen zum Schutzstatus.....15
Ersetzen von Computern.....381
Erstellen der Inhaltsklass.gruppe e. Benutzers..... 246, 261, 265
Erstellen eines Administratorkontos27, 28
Erstellen eines verwalteten Netzwerks ..61
ESS (Extended Service Set) 410
Externe Festplatte.....410

F

Fehler bei der Schlüsselrotation.....370
Fehler durch doppelte Administratoren 369

Festlegen der Cookie-Blockierungsebene eines Benutzers 248, 249, 263
Festlegen der Dateitypen für die Archivierung 284
Festlegen der Internet-Zugriffszeiten eines Benutzers 256
Festlegen von Archivoptionen.....282
Filtern von Nachrichten mit Zeichensätzen 219
Firewall.....410
Firewall sofort sperren 144
Firewall sperren und wiederherstellen 144
Firewall starten 125
Firewall-Schutz aktivieren 125
Firewall-Schutz deaktivieren 126
Firewall-Schutz konfigurieren.....133
Firewall-Sicherheit optimieren 140
Firewall-Sicherheitsstufen verwalten ..134
Firewall-Sperre sofort aufheben.....144
Firewall-Standardeinstellungen wiederherstellen.....145
Fragen und Antworten (FAQs).....116, 240
Freigabe einer Datei 394
Freigabe einer Datei aufheben 395
Freigabe eines Druckers aufheben.....400
Freigeben 411
Freigegebene Datei kopieren.....395
freigegebenes Geheimnis.....411
Funktionen.....10, 46, 52, 58, 78, 122, 198, 244, 280, 300, 384

G

Geschützte drahtlose Netzwerke einrichten 306
Geschützte drahtlose Netzwerke erstellen 308, 333, 371
Geschützte drahtlose Netzwerke überwachen 360, 361, 362, 364
Geschützte drahtlose Netzwerke umbenennen 328, 331
Geschützte drahtlose Netzwerke verlassen 334, 335, 336, 372
Geschützte drahtlose Netzwerkereignisse ansehen..... 360, 361, 362, 363, 364
Gesperrte Computerverbindung bearbeiten.....175
Gesperrte Computerverbindung entfernen 176
Gesperrte Computerverbindung hinzufügen.....174
Gewähren von Zugriff für einen unbekannten Computer 372
Globale Portaktivität anzeigen 185
Grundlagen zum Verwalten persönlicher Filter.....222
Grundlegendes zu Sicherheitswarnungen 82, 113, 116
Grundlegendes zu SystemGuards.....89
Grundlegendes zum Verwalten von Freunden 210

H

Hackerwatch-Lernprogramm starten..196
Hinzufügen einer Website zur Liste der abgelehnten Cookies eines Benutzers 253
Hinzufügen einer Website zur Liste der akzeptierten Cookies eines Benutzers 250
Hinzufügen eines Kennworts zum Kennwort-Tresor.....274
Hinzufügen eines POP3- oder MSN/Hotmail-Web-Mail-Kontos.....202
Hinzufügen von Adressbüchern 212
Hinzufügen von Computern mithilfe der Windows Connect Now-Technologie 320, 321, 349, 368
Hinzufügen von Computern über Wechselgeräte 319, 322, 368
Hinzufügen von persönlichen Filtern..222
Hinzufügen von Web-Mail-Konten 202
Hotspot 411

I

Info zu Browser-SystemGuards.....94
Info zu McAfee.....423
Info zu Windows SystemGuards 91
Info zum Diagramm..... 192, 193
Informationen für drahtlose Geräte ändern..... 331, 341, 370
Informationswarnungen verbergen.....132
Informationswarnungen verwalten.....131
Inhaltsklassifikationsgruppen.....411
Installieren der McAfee-Sicherheits-Software auf Remote-Computern 76
Installieren eines verfügbaren Netzwerkdruckers.....401
Installieren von Wireless Network Security.....366
Instant Messaging-Schutz aktivieren...100
Instant Messaging-Schutz deaktivieren 100
integriertes Gateway 411
Internet 411
Internetdatenverkehr überwachen.....190, 191

Internetverkehr verfolgen 186, 188, 189
Internetzugriff für Programme blockieren 155
Internetzugriff für Programme gewähren 148
Intranet.....411
Intrusion Detection-Ereignisse anzeigen 184
IP-Adresse 412
IP-Spoofing 412
isolieren.....412
Ist zur Ausführung einer Prüfung eine Internetverbindung erforderlich? 116

K

Kann ich VirusScan mit den Browsern 116
Kennwort.....412
Kennwort-Tresor 412
Knoten.....412
Kompatibler drahtloser Adapter wird nicht erkannt 367
Komponenten fehlen oder sind beschädigt.....119
Komprimierung 413
Konfiguration des Echtzeitschutzes.83, 84
Konfigurieren der Update-Optionen 31
Konfigurieren der zu prüfenden Dateitypen 104
Konfigurieren der zu prüfenden Speicherorte 105
Konfigurieren des Echtzeit-Schutzes 84
Konfigurieren des Phishing-Schutzes ..235
Konfigurieren des Schutzstatus.....26
Konfigurieren ignorierter Probleme.....26
Konfigurieren manueller Prüfungen ...102, 104
Konfigurieren von Alarmoptionen 37
Konfigurieren von Benutzeroptionen ...27, 29
Konfigurieren von Informationswarnungen 38
Konfigurieren von SecurityCenter-Optionen 25
Konfigurieren von Sicherheitseinstellungen 338, 381
Konfigurieren von SystemGuards 88
Konfigurieren von Warnoptionen 37
Kopfzeile.....413

L

LAN (Local Area Network) 413

M

MAC (Media Access Control oder Message Authenticator Code) 413
MAC-Adresse (Media Access Control Address) 413
Manuelles Ausführen einer Archivierung 289
Manuelles Beheben von Sicherheitsproblemen 21
Manuelles Hinzufügen von Freunden .210
Manuelles Hinzufügen von Freunden in der SpamKiller-Symbolleiste 210
Manuelles Importieren von Adressbüchern 212
Manuelles Prüfen auf Updates 34, 36
Manuelles Prüfen des Computers 101
Manuelles Scannen 102
Manuelles Warten Ihres Computers 42
MAPI-Konto 413
Markieren von Nachrichten als Spam oder Nicht-Spam von der SpamKiller-Symbolleiste aus 234
McAfee Data Backup.....279
McAfee EasyNetwork 383
McAfee Network Manager 57
McAfee Personal Firewall 121
McAfee Privacy Service 243
McAfee QuickClean.....45
McAfee SecurityCenter 9
McAfee Shredder 51
McAfee SpamKiller.....197
McAfee Total Protection 7
McAfee VirusScan.....77
McAfee Wireless Network Security 299
Mehrere drahtlose Adapter 368
Melden von Spam-Nachrichten.....220
Mit der Statistik arbeiten 185
Mit freigegebenen Druckern arbeiten .400
Mit Warnungen arbeiten 127
MSN-Konto.....413

N

Nachrichten mit Zeichensätzen filtern 219
Netzwerk.....413
Netzwerk scheint ungeschützt 371
Netzwerk umbenennen 63, 390
Netzwerkinformationen eines Computers erhalten.....187
Netzwerk-Laufwerk.....414
Netzwerkschlüssel löschen.....352
Netzwerkschlüssel manuell rotieren ..349, 361, 374
Netzwerkschlüssel verwalten 343, 361

Netzwerk-Sicherheitseinstellungen konfigurieren 340
Netzwerk-Sicherheitseinstellungen reparieren 331, 340, 342, 370, 376
Netzwerksicherheitsmodus ansehen .. 325, 340, 356, 381
Netzwerkverbindungsgeschwindigkeit ansehen 354, 355, 356, 357, 358, 359
Netzwerkzugriffsrechte aufheben 307, 316, 331, 334, 335, 336
Netzwerkzuordnung 414
Netzwerkzuordnung aktualisieren 63
Neuen Systemdienstport konfigurieren 163
NIC (Network Interface Card, Netzwerkkarte) 414
Nicht unterstützter Router oder Zugriffspunkt 369
Nur ausgehenden Zugriff aus dem Protokoll 153, 154, 183
Nur Empfehlungen anzeigen 139

O

Öffnen des Konfigurationsbereichs für . 17, 18, 19, 20
Öffnen des SecurityCenter-Konfigurationsbereichs 22
Öffnen einer archivierten Datei 294
Öffnen von SecurityCenter und Verwenden der zusätzlichen Funktionen 13
Online-Sicherheitsbericht ansehen 354, 355, 356, 357, 358, 359, 367
Online-Sicherungs-Repository 414

P

Parental controls 414
PCI-Drahtlosadapter-Karte 414
Phishing 414
Phishing-Filteroptionen ändern 237
Planen von automatischen Archivierungen 288
Planen von Prüfungen 105
POP3-Konto 414
Popups 414
Potentiell unerwünschtes Programm .. 415
PPPoE 415
Problembehandlung 118, 365
Programmaktivität überwachen 194
Programmbandbreite überwachen 193
Programmberechtigung entfernen 158
Programme und Berechtigungen verwalten 147
Programmen nur den Zugriff auf ausgehende Verbindungen gewähren 152
Programminformationen erhalten 159
Protokoll 415
Protokolle anzeigen 111
Protokollierung, Überwachung und Analyse 179, 189
Proxy 415
Proxy-Server 415
Prüfen des Status Ihrer Updates 14
Prüfen Ihres Schutzstatus 13
Prüfskripte aktivieren 97
Pufferüberlauf 415

R

RADIUS (Remote Access Dial-In User Service) 415
Referenz 403
Regelmäßige Ausdrücke verwenden 225
Registrierungsinformationen eines Computers erhalten 187
Reiner Text 415
Remote-Verwaltung des Netzwerks 71
Reparieren des Routers oder Zugriffspunkts nicht möglich 370
Roaming 415
Router 416

S

Säubern Ihres Computers 49
Scan ohne Verwendung Ihrer Einstellungen für manuelle Scans 103
Scannen in Windows Explorer 103
Schlüssel 416
Schlüssel als Sternchen darstellen 350, 351
Schlüssel automatisch rotieren ... 331, 345, 346, 347, 348, 349, 361, 370, 374
Schlüssel in Klartext anzeigen 350, 351
Schlüsselrotation fortsetzen 345, 346, 349, 374
Schlüsselrotationshäufigkeit anpassen 345, 346, 349
Schnellarchivierung 416
Schutz anderer drahtloser Geräte 309, 317
Schützen oder Konfigurieren des Netzwerks 368
Schützen von Informationen im Internet 267
Schützen von Kennwörtern 273
Schwaches Signal 377
Schwarze Liste 416
Senden von Dateien an andere Computer 397

Server....416
Sicherheit für drahtloses Netzwerk verwalten....337
Sicherheitslücken schließen....75
Sicherheitsmodi konfigurieren....338
sichern....416
Signalstärke des Netzwerks ansehen ..325, 358, 377
Skript....416
Skriptprüfungen deaktivieren....97
SMTP-Server....416
So verfolgen Sie einen Netzwerkcomputer geografisch:....186
Software funktioniert nach Aktualisierung des Betriebssystems nicht....382
Sortieren von archivierten Dateien....292
Spam-Nachrichten melden....220
Speicherort für die oberflächliche Überwachung....417
Speicherort für umfassende Überwachung....417
Sperren von Computerverbindungen..173
SSID (Service Set Identifier)....417
SSL (Secure Sockets Layer)....417
Standard-E-Mail-Konto....417
Starten von EasyNetwork....386
Statistiken zu den globalen Sicherheitsereignissen anzeigen....185
Statuseinstellungen für den Firewall-Schutz konfigurieren....143
Stichwort....417
Stoppen der Überwachung des Schutzstatus eines Computers....73
Suchen nach einer archivierten Datei..293
Suchen nach einer freigegebenen Datei....395
Synchronisieren....417
Systemdienste verwalten....161
Systemdienstport bearbeiten....164
Systemdienstport entfernen....165
Systemdienstports konfigurieren....162
SystemGuard....418

T

TKIP (Temporal Key Integrity Protocol)....418
Trojaner....418

U

Über Wireless Network Security-Symbole....324, 355
Über Zugriffstypen....307, 316
Übergehen zur Verwendung von McAfee-Benutzerkonten....27
Überprüft VirusScan auch komprimierte Dateien?....117
Überprüft VirusScan E-Mail-Anlagen? 117
Überpüfung unter Verwendung der Einstellungen für das manuelle Prüfen....102
Überwachen des Schutzstatus eines Computers....72
Überwachen des Status und der Berechtigungen....72
Überwachte Dateitypen....418
Überwachte IP-Adresse verfolgen....190
Überwachungs-Speicherorte....418
Uneingeschränkten Zugriff aus dem Protokoll....150, 151, 183
Uneingeschränkten Zugriff für ein Programm gewähren....148
Unerwünschte Zugriffspunkte....418
Unter Quarantäne gestellte Programme, Cookies und Dateien an McAfee senden....110
Unterbrechen einer automatischen Archivierung....288
URL....418
USB-Drahtlosadapter-Karten....419

V

Verbinden von Computern mit Ihrem Netzwerk....371
Verbindung unterbrochen....374
Verbindung zu geschützten drahtlosen Netzwerken....315, 331, 332
Verbindung zu Netzwerken mit deaktivierter SSID-Übertragung....317
Verbindung zum drahtlosen Netzwerk nicht möglich....375
Verbindung zum geschützten drahtlosen Netzwerk aufheben....331, 334, 335, 336
Verbindung zum Internet kann nicht hergestellt werden....374
Verbindung zum Internet und Netzwerk aufbauen....373
Verbindungsbenachrichtigung anzeigen....332
Verbindungsstatus ansehen 354, 355, 356, 357, 358, 359
Verbindungsverlust bei Geräten....375
Verhindern, dass eine Website Cookies platziert....264
Vernichten unerwünschter Dateien mit Shredder....53
Vernichten von Dateien, Ordnern und Datenträgern....54
Veröffentlichen....419

Verschieben von Updates auf einen späteren Zeitpunkt....33, 35
Verschlüsselung....419
Vertrauenswürdige Computerverbindung bearbeiten....171
Vertrauenswürdige Computerverbindung entfernen....172
Vertrauenswürdige Computerverbindung hinzufügen....169
Vertrauenswürdige Computerverbindungen....168
Vertrauenswürdigen Computer aus dem Protokoll....170, 182
Verw. isolierter Programme, Cookies und Dateien....109, 118
Verwalten der Filterung von Web-Mail-Konten....207
Verwalten des Spam-Schutzes....232
Verwalten des Virenschutzes....81
Verwalten drahtloser Netzwerke....324
Verwalten eines Geräts....74
Verwalten Ihres Netzwerks....44
Verwalten persönlicher Filter....221
Verwalten vertrauenswürdiger Listen..108
Verwalten von Archiven....298
Verwalten von Freunden....209
Verwalten von gefilterten Nachrichten in Web-Mail-Konten....208
Verwalten von SpamKiller....231
Verwalten von VirusScan....107
Verwalten von Warnungen....114
Verwalten von Web-Mail-Konten....201
Verwaltetes Netzwerk....419
Verwaltetes Netzwerk verlassen....391
Verwenden des E-Mail-Schutzes....98
Verwenden des Explorers der lokale Archive....292
Verwenden des Instant Messaging-Schutzes....100
Verwenden des Menüs....23
Verwenden des Spyware-Schutzes....86
Verwenden des Virenschutzes....82
Verwenden regulärer Ausdrücke....225
Verwenden von QuickClean....49
Verwenden von SecurityCenter....11
Verwenden von Shredder....54
Verwenden von Skriptprüfungen....97
Verwenden von Symbolleisten....233
Verwenden von SystemGuards....87
Virenschutz deaktivieren....82
Vollständige Archivierung....419
Vollständigen Zugriff für ein neues Programm gewähren....149
VPN (Virtual Private Network)....419

W

Wardriver....419
Warneinstellungen konfigurieren....329
Warnungen während eines Spiels anzeigen....131
Warten auf Autorisierung....372
Warum treten bei der Prüfung ausgehender E-Mails Fehler auf?....117
Was sind POP3-, MSN/Hotmail- und MAPI-Konten?....240
Web-Bugs....419
Weiße Liste....419
Weitere Informationen zu Internet Security....195
Weitere Informationen zu Programmen abrufen....159
Weitere Informationen zu Viren....44
Weitere Programminformationen aus dem Protokoll....160, 183
WEP (Wired Equivalent Privacy)....420
Weshalb verwendet McAfee Cookies?..241
Wiederherstellen....420
Wiederherstellen einer älteren Version einer Datei aus einem lokalen Archiv....296
Wiederherstellen von archivierten Dateien....295
Wiederherstellen von fehlenden Dateien aus einem lokalen Archiv....296
Wiederherstellen von unter Quarantäne gestellten Programmen, Cookies und Dateien....109
Wi-Fi (Wireless Fidelity)....420
Wi-Fi Alliance....420
Wi-Fi Certified....420
Windows unterstützt keine drahtlose Verbindung....378
Windows zeigt keine Verbindung an...378
Wireless Network Security deaktivieren....303
Wireless Network Security starten302, 375
WLAN (Wireless Local Area Network)..420
Wörterbuchangriff....421
Wozu dient der Phishing-Filter?....241
WPA (Wi-Fi Protected Access)....421
WPA2....421
WPA2-PSK....421
WPA-PSK....421
Wurm....421

Z

Zugreifen auf die Netzwerkzuordnung..62

Zugriff auf ausgehende Verbindungen für ein Programm gewähren 152
Zugriff auf das Netzwerk gewähren.....389
Zugriff auf einen vorhandenen Systemdienstport gewähren.....162
Zugriff auf einen vorhandenen Systemdienstport sperren 162
Zugriff aus dem Protokoll 157
Zugriff für ein neues Programm sperren 156
Zugriff für ein Programm sperren 155
Zugriffsberechtigungen für Programme entfernen 158
Zugriffspunkt 421
Zulassen einer Website 261
Zulassen von Websites 246, 261
Zulassen, dass eine Website Cookies platziert.....263
Zulassen, dass Websites Cookies platzieren.....263
Zuletzt aufgetretene Ereignisse anzeigen 40, 181
Zurücksetzen des Kennworts für den Kennwort-Tresor.....277
Zurücksetzen Ihres Computers auf die vorherigen Einstellungen 43
Zusätzliche Hilfe.....115, 239